Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук

Кафедра «Защита информации»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2017 г.

Защита автоматизированной системы обработки персональных данных на предпрятии ООО "Диалог-комплект"

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

Автор проекта,
студент группы КЭ- 501
_____ Колпаков, А. Л.
_____ 2017 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2017 г.

Челябинск 2017

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АПКШ – аппаратно-программный комплекс шифрования;
АРМ – автоматизированное рабочие место;
АС – автоматизированная система;
ВТСС – вспомогательные технические средства и системы;
ЗИ – защита информации;
ИБ – информационная безопасность;
ИС – информационная система;
ИСПДн – информационная система персональных данных;
ИТ – информационные технологии;
МСЭ – межсетевой экран;
НСД – несанкционированный доступ;
ООО – Общество с ограниченной ответственностью;
ОТСС – основные технические средства и системы;
ПАК – программно-аппаратный комплекс;
ПДн – персональные данные;
ПО – программное обеспечение;
РД – руководящие документы;
РФ – Российская Федерация;
СВТ – средства вычислительной техники;
СДЗ – средство доверенной загрузки;
ФЗ – Федеральный закон;
ФСБ – Федеральная служба безопасности;
ФСТЭК – Федеральная служба по техническому и экспортному контролю;

Базовые угрозы информационной безопасности – нарушение конфиденциальности, нарушение целостности и отказ в обслуживании;

Ресурс – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер). Свойствами ресурса являются: перечень угроз, воздействующих на него, и критичность ресурса;

Угроза – действие, которое потенциально может привести к нарушению безопасности. Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза;

Уязвимость – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы. Свойствами уязвимости являются: вероятность (простота) реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость;

Критичность ресурса – степень значимости ресурса для информационной системы, т.е. как сильно реализация угроз информационной безопасности на ресурс повлияет на работу информационной системы. Задается в деньгах;

Критичность реализации угрозы – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах;

Вероятность реализации угрозы через данную уязвимость в течение года – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Указывается в процентах.

ВВЕДЕНИЕ

Обработка информации, на сегодняшний день, является одним из наиболее трудоемких процессов, особенно если эта информация ограниченного доступа. Скорость обработки информации и качество получаемых результатов, являются важными факторами, обеспечивающими конкурентоспособность фирмы, а результаты могут являться одним из ценнейших активов организации.

Не представляется возможным представить деятельность предприятия без обработки информации о людях. Обрабатываются данные о сотрудниках, контрагентах, партнерах, акционеров и т.д. Вся эта информация является персональными данными. Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 установлены требования к защите персональных данных при их обработке в информационных системах. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора. Выбор средств защиты информации для системы осуществляется оператором в соответствии с нормативными правовыми актами.

Таким образом, актуальность данной работы обусловлена необходимостью разработки защиты автоматизированной систем обработки персональных данных в ООО «Диалог-комплект».

Объектом выпускной квалификационной работы является ООО «Диалог-комплект».

Предметом выпускной квалификационной работы является автоматизированная система обработки персональных данных в данной организации.

Целью дипломной работы является выбор и обоснование мер по защите автоматизированной системы обработки персональных данных.

В соответствии с поставленной целью необходимо решить следующие задачи:

1. Проанализировать информационную систему ООО «Диалог-комплект», с целью обоснования необходимости создания системы защиты автоматизированной системы обработки персональных данных;
2. Провести анализ и теоретическое обоснование выбора средств защиты информации;
3. Разработать проект по созданию системы защиты автоматизированной системы обработки персональных данных в ООО «Диалог-комплект».

1. АНАЛИЗ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ООО «ДИАЛОГ-КОМПЛЕКТ» И СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ

1.1. Разработка технического паспорта

Для создания системы защиты информации было проведено предпроектное обследование предприятия, в результате которого был составлен технический паспорт (Приложение А).

В техническом паспорте приведен состав ОТСС, ВТСС, схемы их размещения, расположение линий коммуникаций, перечень установленных средств защиты информации и программного обеспечения.

В качестве объекта защиты была выбрана АС «КЛИЕНТЫ» ООО «Диалог-комплект».

1.2. Разработка модели деятельности

В ходе обследования работы АС «КЛИЕНТЫ» была построена модель деятельности (Приложение Ж). В этой схеме отражаются основные этапы технологического процесса обработки защищаемой информации от подготовки к обработке информации ограниченного доступа до сохранения результатов.

Данная модель необходима для выявления потоков информации ограниченного доступа.

1.3. Выявление защищаемой информации

В результате проведенного предпроектного обследования, ознакомления с информацией ограниченного доступа и организационно-распорядительной документацией была выявлена следующая защищаемая информация: Перечень персональных данных, подлежащих защите в автоматизированной системе обработки персональных данных «КЛИЕНТЫ» № 571 от 05.11.2016 г.

В рамках данной ВКР был разработан перечень персональных данных (Приложение В).

1.4. Описание информационной системы

Система защиты информации в АС «КЛИЕНТЫ» ООО «Диалог-комплект» основана на использовании организационных, правовых и программно-аппаратных мер.

Организационные меры включают в себя инструкции администратора, инструкции пользователей, инструкцию по эксплуатации СЗИ, инструкцию по антивирусной, инструкцию по парольной защите, инструкцию по резервированию, журнал учета лиц, журнал учета машинных носителей.

В рамках ВКР была разработана инструкция по антивирусной защите (Приложение Г). Инструкции администратора, инструкции пользователей, инструкция по

эксплуатации СЗИ, инструкция по парольной защите, инструкция по резервированию, журнал учета лиц, журнал учета машинных носителей ранее существовали на предприятии.

Правовые меры включают в себя нормативно-правовые документы, регулирующие деятельность организации в области обеспечения защиты информации:

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [1];

– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [6];

– Федеральный закон «О персональных данных» [15];

– Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [7];

– Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [8].

Программно-аппаратные меры включают в себя комплекс программно-аппаратных средств, обеспечивающих работу автоматизированной системы и ее защиту. В рамках ВКР была проведена инвентаризация автоматизированной системы, результаты которой представлены в Таблицах 1 и 2.

Таблица 1 – Аппаратное обеспечение

Наименование устройства	Фирма производитель, модель	Заводской / инвентаризационный номер
1	2	3
ОТСС		
Системный блок	InWin	16112060900152
НЖМД	WD WD3200AAKX-001CA0	WD-WCAYUAA20921
Монитор	LG L1942S-BF	907NDBP3G709
Клавиатура	Genius K639	ZM7902171374
Мышь	A4-Tech OP-620D	0907
Принтер	HP LaserJet 1018	CNC1L86960
ИБП	APC SmartuPS 500	QS0614121487
ВТСС		
Системный блок	InWin	619G109000187
Монитор	Samsung SyncMaster 720 NA	GS17HVFLA00045F
Клавиатура	Oklick 320M	3922302126
Мышь	Genius GM-0003A	X62405206687
МФУ	Canon MF3110	VZN81841
Системный блок	InWin	16221034300108
Монитор	LG	BEJE2241SX

Продолжение таблицы 1

1	2	3
Клавиатура	Logitech-k200	SY1464K
МФУ	HP LaserJet M1005MFP	CNG87CKHUF
Мышь	Logitech B110	LZ137HR21NP
Телефонный аппарат	LG GS0472H	
Телефонный аппарат	LG GS0472H	
Крипто-маршрутизатор	АПКШ континент	CH010105
Датчик пожарной сигнализации	б/н	
Датчик пожарной сигнализации	б/н	
Коммутатор	D-link DES-1005D	B12D449021069

Таблица 2 – Программное обеспечение

Наименование	Версия
Microsoft Windows 7 Professional SP1	6.1.7601.17514
7-zip	9.20.00.0
DallasLock 8.0-K	8.0.347.4
Kaspersky Endpoint Security 10 для Windows	10.2.5.3201
АРМ «Феанор»	10.63
КриптоПро CSP	3.9.8171

1.5. Выявление объектов защиты

На основе перечня защищаемой информации, изучения модели деятелности и технологического процесса обработки информации были выявлены объекты защиты и составлен их перечень:

– автоматизированное рабочее место, на котором обрабатывается защищаемая информация;
– средства ввода-вывода и отображения информации;
– система бесперебойного питания АРМ;
– линии и средства связи, системы обеспечения функционирования СВТ и деятельности организации;
– носители информации;
– персонал.

Более подробно перечень объектов защиты представлен в Приложении А.

1.6. Разработка модели угроз и уязвимостей для важных объектов защиты

Модель угроз безопасности информации, учитывая особенности информационной системы, используемые в ней программные, программно-технические, технические средства и процессы обработки информации, дает описание угроз безопасности, которым подвержена информационная система.

На основании модели деятельности организации был сформулирован перечень важных объектов защиты:

– персонал;

– автоматизированное рабочее место, на котором обрабатывается защищаемая информация;

Далее, были выделены наиболее существенные угрозы информационной безопасности и разработана модель угроз на основании документа «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)» ФСТЭК.

Подробное описание модели угроз приведено в пунктах 1.6.1., 1.6.2., 1.6.3.

1.6.1. Угрозы несанкционированного доступа к информации

1.6.1.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн

1.6.1.1.1. Кража ПЭВМ

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

В здании ООО «Диалог-комплект» введен круглосуточный контроль доступа в контролируемую зону, который осуществляется частным охранным предприятием, двери, закрываются на замок, вынос компьютерный техники за пределы здания возможен только с разрешения охраны.

Вероятность реализации угрозы – маловероятна.

1.6.1.1.2. Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

В здании ООО «Диалог-комплект» введен контроль доступа в контролируемую зону, двери закрываются на замок, ведется учет и хранение носителей в сейфе.

Вероятность реализации угрозы – маловероятна.

1.6.1.1.3. Кража ключей и атрибутов доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

В здании ООО «Диалог-комплект» введен контроль доступа в контролируемую зону, двери закрываются на замок, организовано хранение ключей и паролей в сейфе и введена политика «чистого стола».

Вероятность реализации угрозы – маловероятна.

1.6.1.1.4. Кража, модификация, уничтожение информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

В здании ООО «Диалог-комплект» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна.

1.6.1.1.5. Вывод из строя узлов ПЭВМ, каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

В здании ООО «Диалог-комплект» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна.

1.6.1.1.6. Несанкционированный доступ к информации при технческом обслуживании (ремонте, уничтожении) узлов ПЭВМ

В Учреждении техническое обслуживание ПЭВМ осуществляется сотрудниками, подписавшими соглашение о неразглашении.

Вероятность реализации угрозы – маловероятна.

1.6.1.1.7. Несанкционированное отключение средств защиты

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.

В здании ООО «Диалог-комплект» введен контроль доступа в контролируемую зону, двери закрываются на замок, пользователи ИСПДн проинструктированы о работе с ПДн.

Вероятность реализации угрозы – низкая вероятность.

1.6.1.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)

1.6.1.2.1. Действия вредоносных программ (вирусов)

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

– скрывать признаки своего присутствия в программной среде компьютера;

– обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

– разрушать (искажать произвольным образом) код программ в оперативной памяти;

– выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

– сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

– искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Необходимо установить антивирусное программное обеспечение и проинструктировать персонал об антивирусной защите.

Вероятность реализации угрозы – высокая вероятность.

1.6.1.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Разработку и сопровождение программного обеспечения ИСПДн осуществляет доверенная организация.

Вероятность реализации угрозы – маловероятна.

1.6.1.2.3. Установка ПО, не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

Все пользователи проинструктированы о политике установки ПО и осуществляется контроль.

Вероятность реализации угрозы – средняя вероятность.

1.6.1.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п) характера

1.6.1.3.1. Утрата ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политике в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

В учреждении введена парольная политика, предусматривающая требуемую сложность пароля, введена политика «чистого стола», осуществляется контроль за их выполнением, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей.

Вероятность реализации угрозы – средняя вероятность.

1.6.1.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не осведомлены о них.

В учреждении резервное копирование обрабатываемых ПДн не осуществляется.

Вероятность реализации угрозы – высокая вероятность.

1.6.1.3.3. Непреднамеренное отключение средств защиты

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

В учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПДн.

Требуется установка ПАК для доверенной загрузки.

Вероятность реализации угрозы – высокая вероятность.

1.6.1.3.4. Выход из строя аппаратно-программных средств

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

В учреждении осуществляется резервирование ключевых элементов ИСПДн.

Вероятность реализации угрозы – средняя вероятность.

1.6.1.3.5. Сбой системы электроснабжения

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

В учреждении ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания.

Вероятность реализации угрозы – маловероятна.

1.6.1.3.6. Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

В учреждении установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – маловероятна.

1.6.2. Угрозы преднамеренных действий внутренних нарушителей

1.6.2.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

В здании ООО «Диалог-комплект» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна.

1.6.2.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

В учреждении пользователи осведомлены о порядке работы с персональными данными, а также подписали Соглашение о неразглашении.

Требуется резервное копирование, обрабатываемой информации, требуется установка СЗИ от НСД, требуется установка антивирусной защиты.

Вероятность реализации угрозы – высокая вероятность.

1.6.3. Угрозы несанкционированного доступа по каналам связи

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (п. 6.6. Базовой модели угроз безопасности персональных данных при их обработке в инфор-

мационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г.), для ИСПДн можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

– угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;

– угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;

– угрозы выявления паролей по сети;

– угрозы навязывания ложного маршрута сети;

– угрозы подмены доверенного объекта в сети;

– угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

– угрозы типа «Отказ в обслуживании»;

– угрозы удаленного запуска приложений;

– угрозы внедрения по сети вредоносных программ.

1.6.3.1. Угроза «Анализ сетевого траффика»

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель:

– изучает логику работы ИСПДн - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;

– перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.

В ИСПДн осуществляется передача информации по каналам связи с использованием криптошлюза.

Вероятность реализации угрозы – маловероятна.

1.6.3.2. Угроза «сканирование сети»

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель – выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

В ИСПДн осуществляется передача информации по каналам связи с использованием криптошлюза.

Вероятность реализации угрозы – маловероятна.

1.6.3.3. Угроза выявления паролей

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

В учреждении применяются стойкие пароли согласно Руководящему документу «Автоматизированные системы…».

Вероятность реализации угрозы – маловероятна.

1.6.3.4. Угрозы навязывания ложного маршрута сети

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализации угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

В ИСПДн межсетевое взаимодействие осуществляется посредством криптошлюза.

Вероятность реализации угрозы – маловероятна.

1.6.3.5. Угрозы подмены доверенного объекта

Такая угроза эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа к техническому средству ИСПДн - цели угроз.

В ИСПДн межсетевое взаимодействие осуществляется посредством криптошлюза.

Вероятность реализации угрозы – маловероятна.

1.6.3.6. Внедрение ложного объекта сети

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

В ИСПДн межсетевое взаимодействие осуществляется посредством криптошлюза.

Вероятность реализации угрозы – маловероятна.

1.6.3.7. Угрозы типа «Отказ в обслуживании»

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

– скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;

– явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);

– явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;

– явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений.

Вероятность реализации угрозы – маловероятно.

1.6.3.8. Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

– распространение файлов, содержащих несанкционированный исполняемый код;

– удаленный запуск приложения путем переполнения буфера приложений-серверов;

– удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений.

Вероятность реализации угрозы – маловероятно.

1.6.3.9. Угрозы внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

– программы подбора и вскрытия паролей;

– программы, реализующие угрозы;

– программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;

– программы-генераторы компьютерных вирусов;

– программы, демонстрирующие уязвимости средств защиты информации и др.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений.

Вероятность реализации угрозы – маловероятно.

1.7. Расчет рисков важных объектов защиты

Расчет рисков важных объектов защиты предприятия ООО «Диалог-комплект» был выполнен на основе документа «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК.

1.7.1 Вероятность реализации угроз безопасности персональных данных

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

– маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);

– низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);

– средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);

– высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

1.7.2 Реализуемость угроз

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В Таблице 4 представлены характеристики уровня исходной защищенности для ИСПДн.

Таблица 3 – Исходный уровень защищенности

Технические и эксплуатационные характеристики	Уровень защищенности
1	2
По территориальному размещению	Высокий
По наличию соединения с сетями общего пользования	Средний
По встроенным (легальным) операциям с записями баз персональных данных	Низкий

Продолжение таблицы 3

1	2
По разграничению доступа к персональным данным	Средний
По наличию соединений с другими базами ПДн иных ИСПДн	Средний
По уровню (обезличивания) ПДн	Низкий
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	Высокая

ИСПДн имеет средний уровень исходной защищенности, так как не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний».

Показатель исходной защищенности Y1 = 5.

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20

Оценка реализуемости угроз безопасности персональных представлена в Таблице 4.

Таблица 4 – Реализуемость угроз

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1	2	3
Угрозы несанкционированного доступа к информации		
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
Кража ПЭВМ	0,25	низкая
Кража носителей информации	0,25	низкая
Кража ключей и атрибутов доступа	0,25	низкая
Кражи, модификации, уничтожения информации	0,25	низкая
Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
Несанкционированное отключение средств защиты	0,35	средняя
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)		

Продолжение таблицы 4

1	2	3
Действия вредоносных программ (вирусов)	0,75	высокая
Недекларированные возможности системного ПО и ПО для обработки персональных данных	0,25	низкая
Установка ПО не связанного с исполнением служебных обязанностей	0,5	средняя
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера		
Утрата ключей и атрибутов доступа	0,5	средняя
Непреднамеренная модификация (уничтожение) информации сотрудниками	0,75	высокая
Непреднамеренное отключение средств защиты	0,75	высокая
Выход из строя аппаратно-программных средств	0,5	средняя
Сбой системы электроснабжения	0,25	низкая
Стихийное бедствие	0,25	низкая
Угрозы преднамеренных действий внутренних нарушителей		
Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	0,25	низкая
Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	0,75	высокая
Угрозы несанкционированного доступа по каналам связи		
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	0,25	низкая
Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0,25	низкая
Угрозы выявления паролей по сети	0,25	низкая
Угрозы навязывание ложного маршрута сети	0,25	низкая

Продолжение таблицы 4

1	2	3
Угрозы подмены доверенного объекта в сети	0,25	низкая
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,25	низкая
Угрозы типа «Отказ в обслуживании»	0,25	низкая
Угрозы удаленного запуска приложений	0,25	низкая
Угрозы внедрения по сети вредоносных программ	0,25	низкая

1.7.3 Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

– низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

– средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

– высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности угроз безопасности персональных данных представлена в Таблице 5.

Таблица 5 – Опасность угроз персональных данных

Тип угроз безопасности ПДн	Опасность угрозы
1	2
Угрозы несанкционированного доступа к информации	
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
Кража ПЭВМ	Низкая
Кража носителей информации	Низкая
Кража ключей и атрибутов доступа	Низкая
Кражи, модификации, уничтожения информации	Низкая
Вывод из строя узлов ПЭВМ, каналов связи	Низкая
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Низкая
Несанкционированное отключение средств защиты	Низкая

Продолжение таблицы 5

1	2
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)	
Действия вредоносных программ (вирусов)	Низкая
Недекларированные возможности системного ПО и ПО для обработки персональных данных	Низкая
Установка ПО не связанного с исполнением служебных обязанностей	Низкая
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера	
Утрата ключей и атрибутов доступа	Низкая
Непреднамеренная модификация (уничтожение) информации сотрудниками	Низкая
Непреднамеренное отключение средств защиты	Низкая
Выход из строя аппаратно-программных средств	Низкая
Сбой системы электроснабжения	Низкая
Стихийное бедствие	Низкая
Угрозы преднамеренных действий внутренних нарушителей	
Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	Низкая
Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Низкая
Угрозы несанкционированного доступа по каналам связи	
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	Низкая
Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	Низкая
Угрозы выявления паролей по сети	Низкая
Угрозы навязывание ложного маршрута сети	Низкая
Угрозы подмены доверенного объекта в сети	Низкая
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	Низкая
Угрозы типа «Отказ в обслуживании»	Низкая
Угрозы удаленного запуска приложений	Низкая
Угрозы внедрения по сети вредоносных программ	Низкая

1.7.4 Определение актуальности угроз

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

Таблица 6 – Определение актуальности угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Оценка актуальности угроз безопасности представлена в Таблице 7.

Таблица 7 – Актуальность угроз безопасности персональных данных

Тип угроз безопасности ПДн	Актуальность угрозы
1	2
Угрозы несанкционированного доступа к информации	
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
Кража ПЭВМ	Не актуальная
Кража носителей информации	Не актуальная
Кража ключей и атрибутов доступа	Не актуальная
Кражи, модификации, уничтожения информации	Не актуальная
Вывод из строя узлов ПЭВМ, каналов связи	Не актуальная
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Не актуальная
Несанкционированное отключение средств защиты	Не актуальная
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)	
Действия вредоносных программ (вирусов)	Актуальная
Недекларированные возможности системного ПО и ПО для обработки персональных данных	Не актуальная
Установка ПО не связанного с исполнением служебных обязанностей	Не актуальная

Продолжение таблицы 7

1	2
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера	
Утрата ключей и атрибутов доступа	Не актуальная
Непреднамеренная модификация (уничтожение) информации сотрудниками	Актуальная
Непреднамеренное отключение средств защиты	Актуальная
Выход из строя аппаратно-программных средств	Не актуальная
Сбой системы электроснабжения	Не актуальная
Стихийное бедствие	Не актуальная
Угрозы преднамеренных действий внутренних нарушителей	
Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	Не актуальная
Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Актуальная
Угрозы несанкционированного доступа по каналам связи	
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	Не актуальная
Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	Не актуальная
Угрозы выявления паролей по сети	Не актуальная
Угрозы навязывание ложного маршрута сети	Не актуальная
Угрозы подмены доверенного объекта в сети	Не актуальная
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	Не актуальная
Угрозы типа «Отказ в обслуживании»	Не актуальная
Угрозы удаленного запуска приложений	Не актуальная
Угрозы внедрения по сети вредоносных программ	Не актуальная

1.8. Разработка технического задания на создание системы защиты персональных данных на предприятии ООО «Диалог-комплект»

По результатам предпроектного обследования было разработано техническое задание на создание системы защиты персональных данных на предприятии ООО «Диалог-комплект» (Приложение Б).

В качестве основы был взят ГОСТ 34.602-1989 «Техническое задание на создание автоматизированной системы» [2]. Техническое задание имеет следующие разделы:

1) общие сведения.
2) назначение и цели совершенствования системы;
3) характеристика объектов защиты;
4) требования к ИСПДн;
5) состав и содержание работ по совершенствованию системы;
6) порядок контроля и приемки системы;
7) требования к составу и содержанию работ по подготовке объекта защиты к вводу ИСПДн в действие;
8) требования к документированию;
9) источники разработки.

1.9. Безопасность жизнедеятельности

Безопасность жизнедеятельности – это система организационных мероприятий и технических средств, предотвращающих воздействие на работающих опасных производственных факторов. При приеме на работу будущий сотрудник обязательно должен пройти вводный инструктаж и первичный инструктаж на рабочем месте. Руководители предприятий и их подразделений осуществляют четкий контроль над своевременными инструктажами. Обязательно ведут журнал, где ставят подписи все работники, которые прошли инструктаж.

Потенциально опасные и вредные производственные факторы являются важными показателями при организации рабочего места. Классификацию этих факторов обозначены в Трудовом кодексе Российской Федерации.

Вредный производственный фактор - производственный фактор, воздействие которого на работника может привести к его заболеванию.

Опасный производственный фактор - производственный фактор, воздействие которого на работника может привести к его травме.

Условия труда пользователя, работающего с персональным компьютером, определяются:

– особенностями организации рабочего места;
– условиями производственной среды;
– характеристиками информационного взаимодействия человека и персональных электронно-вычислительных машин.

1.9.1. Рекомендации по организации рабочего места пользователя

Рассмотрим основные нормативные документы и приведем некоторые рекомендации по организации рабочего места пользователя.

1.9.1.1. Рекомендации по выбору помещения для размещения рабочего места

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное помещение, в котором будут располагаться рабочие места, оборудование ЭВМ с ВДТ.

По требованиям СанПиН 2.2.2/2.4.1340-03 [9] помещения для эксплуатации ПЭВМ должны отвечать следующим требованиям:

– помещения должны иметь естественное и искусственное освещение;

– естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации;

– площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные), по СанПиН 2.2.2/2.4.1340-03, должно быть– 4,5 м^2 и 6 м^2 для ВДТ на базе ЭЛТ;

– для внутренней отделки интерьера помещений, где расположены ПЭВМ, должны использоваться диффузно-отражающие материалы с коэффициентом отражения для потолка – 0,7−0,8; для стен – 0,5−0,6; для пола – 0,3−0,5;

– помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным занулением или заземлением в соответствии с техническими требованиями по эксплуатации;

– не допускается расположение рабочих кабинетов, оборудованных ПЭВМ, в полуподвальных и подвальных помещениях.

Не следует размещать рабочие места с ПЭВМ вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, чтобы избежать появления помех, нарушающих функционирование ПЭВМ.

1.9.1.2. Требования к микроклимату

Для рабочих мест, на которых работа с ПЭВМ является основным видом выполняемых работ и связана с непрерывным эмоциональным напряжением, согласно СанПиН 2.2.2/2.4.1340-03 должны быть обеспечены оптимальные параметры микроклимата для работ категории Iа (Таблица 8). Параметры требований к микроклимату для работ различных категорий приведены в СанПиН 2.2.4.3359-16 [11].

Таблица 8 – Гигиенические требования к микроклимату производственных помещений (СанПиН 2.2.4.3359-16).

Период года	Категория работ по уровням энергозатрат, Вт	Температура воздуха, °С	Температура поверх-ностей, °С	Относи-тельная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	Iа (до 139)	22 – 24	21 – 25	60 – 40	0,1
Теплый	Iа (до 139)	23 – 25	22 – 26	60 – 40	0,1

В соответствии с СанПиН 2.2.4.3359-16, в помещениях, оборудованных ПЭВМ, должна проводиться ежедневная влажная уборка, а также проветривание после каждого часа работы на ПЭВМ.

1.9.1.3. Требования к уровням шума

При работе на ПЭВМ источниками шума являются:

- источник бесперебойного питания;
- системный блок ПЭВМ;
- работающие принтеры и многофункциональные устройства.

Уровень шума на рабочих местах, при выполнении основных и вспомогательных производственных работ с использованием ПЭВМ не должен превышать показателей, устанавливаемых нормами СанПиН 2.2.2/2.4.1340-03 предельно допустимых значений для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами. А именно должен соответствовать нормам СанПиН 2.2.4.3359-16 для высококвалифицированной работы, требующей сосредоточенности, в рабочих комнатах.

В соответствии с нормами, ограничивающими предельно допустимое звуковое давление для рабочих мест, оснащённых ПЭВМ: шумящее оборудование, уровни шума которого превышают нормативные, должно размещаться вне помещений с ПЭВМ.

В соответствии с СанПин 2.2.4.3359-16 уровни шума на рабочих местах не должны превышать 80дБА.

1.9.1.4. Требования к освещению

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное освещение, не вызывающее раннего переутомления. Работа программиста требует большой зрительной нагрузки, поэтому необходимо применять естественное освещение совместно с искусственным.

Согласно СанПиН 2.2.2/2.4.1340-03 рабочие столы следует размещать таким образом, чтобы ВДТ были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева. Искусственное освещение в помещениях для эксплуатации ПЭВМ должно осуществляться системой общего равномерного освещения. В производственных и административно-общественных помещениях, в случаях преимущественной работы с документами и бумагами, следует применять системы комбинированного освещения.

Освещенность на поверхности рабочего стола должна быть 300−500 лк. Освещенность поверхности экрана не должна быть более 300 лк., освещение не должно создавать бликов на поверхности экрана.

Для освещения помещений с ПЭВМ рекомендуется применять светильники с зеркальными параболическими решетками, укомплектованными электронными пускорегулирующими аппаратами (ЭПРА). Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя и линии оконных проёмов при рядном расположении рабочих мест, оснащённых ПЭВМ с ВДТ. При периметральном расположении компьютеров линии светильников должны располагаться локализовано над рабочим

столом ближе к его переднему краю, обращенному к оператору. Коэффициент пульсации не должен превышать 5%.

Для обеспечения нормируемых значений освещенности в помещениях для использования ПЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

1.9.1.5. Общие требования к организации рабочих мест

Рабочее место оператора ЭВМ проектируется согласно СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов – не менее 1,2 м.

Рабочие места с ПЭВМ в помещениях с источниками вредных производственных факторов должны размещаться в изолированных кабинах с организованным воздухообменом.

Рабочие места с ПЭВМ при выполнении работы, требующей значительного умственного напряжения или высокой концентрации внимания, рекомендуется изолировать друг от друга перегородками высотой 1,5−2,0 м.

Экран видеомонитора должен находиться от глаз пользователя на расстоянии 600−700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов.

Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы.

При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики. Поверхность рабочего стола должна иметь коэффициент отражения 0,5−0,7.

При организации рабочих мест необходимо использовать рабочий стул (кресло) обеспечивающий поддержание рациональной рабочей позы при работе на ПЭВМ, позволяющий изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ.

Рабочий стул (кресло) должно быть обеспеченно подъемно-поворотным механизмом, также оно должно быть регулируемым по высоте и углам наклона сиденья и спинки, а также расстояния спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию.

Поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений.

Высота рабочей поверхности стола должна регулироваться в пределах 680−800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм.

Модульными размерами рабочей поверхности стола для ПЭВМ, на основании которых должны рассчитываться конструктивные размеры, следует считать: ширину 800, 1000, 1200 и 1400 мм, глубину 800 и 1000 мм при нерегулируемой его высоте, высота должна быть равной 725 мм.

Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной – не менее 500 мм, глубиной на уровне колен – не менее 450 мм и на уровне вытянутых ног – не менее 650 мм.

Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей (размер ВДТ и ПЭВМ, клавиатуры, и др.), характера выполняемой работы. При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики.

Конструкция стула (кресла) должна обеспечивать:

– ширину и глубину поверхности сиденья не менее 400 мм;

– поверхность сиденья с закругленным передним краем;

– регулировку высоты поверхности сиденья в пределах 400−550 мм и углам наклона вперед до 15°, и назад до 5°;

– высоту опорной поверхности спинки 300±20 мм, ширину – не менее 380мм и радиус кривизны горизонтальной плоскости – 400 мм;

– угол наклона спинки в вертикальной плоскости в пределах ±30°;

– регулировку расстояния спинки от переднего края сиденья в пределах 260−400 мм;

– стационарные или съемные подлокотники длиной не менее 250 мм и шириной – 50−70 мм;

– регулировку подлокотников по высоте над сиденьем в пределах 230±30 мм и внутреннего расстояния между подлокотниками в пределах 350−500 мм.

Рабочее место пользователя ПЭВМ, согласно СанПиН 2.2.2.542-96 [10], следует оборудовать подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20°. Поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм.

Клавиатуру следует располагать на поверхности стола на расстоянии 100−300 мм от края, обращенного к пользователю или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

1.9.2. Электробезопасность

По степени опасности поражения электрическим током согласно Правилам Устройства Электроустановок (ПУЭ) рабочее помещение относится к классу помещений с повышенной опасностью, так как имеется возможность одновременного прикосновения человека к имеющим соединения с землей металлоконструкциям здания с одной стороны и металлическим корпусам электрооборудования с другой.

Если физический доступ к токоведущим частям оборудования затруднен, то основной причиной возникновения данного опасного фактора может являться прикосновение к металлическим нетоковедущим частям (например, корпусу ПЭВМ), которые могут оказаться под напряжением в результате повреждения изоляции. В соответствии с правилами электробезопасности, должен осуществляться постоянный контроль состояния электропроводки, предохранительных щитов, шнуров, с помощью которых включаются в электросеть компьютеры, осветительные приборы, другие электроприборы.

Для защиты от случайного прикосновения к металлическим нетоковедущим частям оборудования, которые могут оказаться под напряжение применяют следующие меры:

– защитное заземление;
– зануление;
– изоляцию нетоковедущих частей;
– защитное экранирование.

Данные меры описаны в ГОСТ Р 12.1.019-2009 «ССБТ. Электробезопасность. Общие требования и номенклатура видов защиты» [3].

1.9.3. Пожарная безопасность

Горючие вещества и материалы, находящиеся в помещении: дерево (мебель), бумага (документы), ПЭВМ.

Возможными источниками зажигания могут быть тепловые проявления электрической энергии (короткое замыкание. высокие сопротивления, искровые разряды статического электричества и др.).

Источниками пожара может стать неисправность или нарушение правил эксплуатации электротехнического оборудования.

Для тушения возможного пожара помещение оборудовано одним ручным порошковым огнетушителем ОП-4.

На основе ФЗ «Технический регламент о требованиях пожарной безопасности» были установлены следующие правила:

Организации, их должностные лица и граждане, нарушившие требования пожарной безопасности, несут ответственность в соответствии с законодательством Российской Федерации.

Наряду с настоящими Правилами, следует также руководствоваться иными нормативными документами по пожарной безопасности и нормативными документами, содержащими требования пожарной безопасности, утвержденными в установленном порядке.

Руководители организации и индивидуальные предприниматели на своих объектах должны иметь систему пожарной безопасности, направленную на предотвращение воздействия на людей опасных факторов пожара, в том числе их вторичных проявлений.

На каждом объекте должны быть разработаны инструкции о мерах пожарной безопасности для каждого взрывопожароопасного и пожароопасного участка (мастерской, цеха и т.п.) в соответствии с приложением данных правил.

Все работники организаций должны допускаться к работе только после прохождения противопожарного инструктажа, а при изменении специфики работы проходить дополнительное обучение по предупреждению и тушению возможных пожаров в порядке, установленном руководителем.

Руководители организаций или индивидуальные предприниматели имеют право назначать лиц, которые по занимаемой должности или по характеру выполняемых работ в силу действующих нормативных правовых актов и иных актов должны выполнять соответствующие правила пожарной безопасности либо обеспечивать их соблюдение на определенных участках работ.

Для привлечения работников предприятий к работе по предупреждению и борьбе с пожарами на объектах могут создаваться пожарно-технические комиссии и добровольные пожарные формирования.

Собственники имущества, лица, уполномоченные владеть, пользоваться или распоряжаться имуществом, в том числе руководители и должностные лица организаций, лица, в установленном порядке назначенные ответственными за обеспечение пожарной безопасности, должны:

– обеспечивать своевременное выполнение требований пожарной безопасности, предписаний, постановлений и иных законных требований государственных инспекторов по пожарному надзору;

– создавать и содержать на основании утвержденных в установленном порядке норм, перечней особо важных и режимных объектов и предприятий, на которых создается пожарная охрана, органы управления и подразделения пожарной охраны, а также обеспечивать в них непрерывное несение службы и использование личного состава и пожарной техники строго по назначению.

Во всех производственных, административных, складских и вспомогательных помещениях на видных местах должны быть вывешены таблички с указанием номера телефона вызова пожарной охраны.

Правила применения на территории организаций открытого огня, проезда транспорта, допустимость курения и проведения временных пожароопасных работ устанавливаются общеобъектовыми инструкциями о мерах пожарной безопасности.

В каждой организации распорядительным документом должен быть установлен соответствующий их пожарной опасности противопожарный режим, в том числе:

– определены и оборудованы места для курения;

– определены места и допустимое количество единовременно находящихся в помещениях сырья, полуфабрикатов и готовой продукции;

– установлен порядок уборки горючих отходов и пыли, хранения промасленной спецодежды;

– определен порядок обесточивания электрооборудования в случае пожара и по окончании рабочего дня;

– регламентированы:

– порядок проведения временных огневых и других пожароопасных работ;

– порядок осмотра и закрытия помещений после окончания работы;

– действия работников при обнаружении пожара;

– определен порядок и сроки прохождения противопожарного инструктажа и занятий по пожарно-техническому минимуму, а также назначены ответственные за их проведение.

В зданиях и сооружениях (кроме жилых домов) при единовременном нахождении на этаже более 10 человек должны быть разработаны и на видных местах вывешены планы (схемы) эвакуации людей в случае пожара, а также предусмотрена система (установка) оповещения людей о пожаре.

На объектах с массовым пребыванием людей (50 и более человек) в дополнение к схематическому плану эвакуации людей при пожаре должна быть разработана инструкция, определяющая действия персонала по обеспечению безопасной и быстрой эвакуации людей, по которой не реже одного раза в полугодие должны проводиться практические тренировки всех задействованных для эвакуации работников.

Световая, звуковая и визуальная информирующая сигнализация должна быть предусмотрена в помещениях, посещаемых данной категорией лиц, а также у каждого эвакуационного, аварийного выхода и на путях эвакуации. Световые сигналы в виде светящихся знаков должны включаться одновременно со звуковыми сигналами. Работники организаций, а также граждане должны:

– соблюдать на производстве и в быту требования пожарной безопасности, а также соблюдать и поддерживать противопожарный режим;

– выполнять меры предосторожности при пользовании газовыми приборами, предметами бытовой химии, проведении работ с легковоспламеняющимися (далее - ЛВЖ) и горючими (далее - ГЖ) жидкостями, другими опасными в пожарном отношении веществами, материалами и оборудованием;

– в случае обнаружения пожара сообщить о нем в подразделение пожарной охраны и принять возможные меры к спасению людей, имущества и ликвидации пожара.

Граждане предоставляют в порядке, установленном законодательством Российской Федерации, возможность государственным инспекторам по пожарному надзору проводить обследования и проверки принадлежащих им производственных, хозяйственных, жилых и иных помещений и строений в целях контроля за соблюдением требований пожарной безопасности.

Противопожарные системы и установки (противодымная защита, средства пожарной автоматики, системы противопожарного водоснабжения, противопожарные двери, клапаны, другие защитные устройства в противопожарных стенах и перекрытиях и т.п.) помещений, зданий и сооружений должны постоянно содержаться в исправном рабочем состоянии.

Устройства для самозакрывания дверей должны находиться в исправном состоянии. Не допускается устанавливать какие-либо приспособления, препятствующие нормальному закрыванию противопожарных или противодымных дверей (устройств). Нормы оснащения помещения ручным огнетушителем приведены в Таблице 13.

1.9.4. Рекомендации по организации режима труда и отдыха пользователя

Режимы труда и отдыха при работе с ПЭВМ и ВДТ должны организовываться в зависимости от вида и категории трудовой деятельности согласно СанПиН 2.2.2/2.4.1340-03.

По виду трудовой деятельности работу оператора можно отнести к группе «А» – работа по считыванию информации с экрана ВДТ или ПЭВМ с предварительным запросом.

Для видов трудовой деятельности устанавливается три категории тяжести и напряженности работы с ВДТ и ПЭВМ.

Для группы А категории определяются по суммарному числу считываемых знаков за рабочую смену, но не более 60 000 знаков за смену:

– 1 категория – до 20 000 знаков;
– 2 категория – до 40 000 знаков;
– 3 категория – до 60 000 знаков.

Продолжительность обеденного перерыва определяется действующим законодательством о труде и правилами внутреннего распорядка предприятия.

Для обеспечения оптимальной работоспособности и сохранения здоровья профессиональных пользователей, на протяжении рабочей смены должны устанавливаться регламентированные перерывы. Время регламентированных перерывов в течении рабочей смены следует устанавливать в зависимости от ее продолжительности, вида и категории трудовой деятельности. Продолжительность непрерывной работы без регламентированного перерыва не должна превышать двух часов. При восьмичасовой рабочей смене и работе на ВДТ и ПЭВМ регламентированные перерывы следует устанавливать:

– для 1 категории работ через 2 ч. от начала рабочей смены и через 2 ч. после обеденного перерыва продолжительностью 15 мин. каждый;

– для 2 категории работ через 2 ч. от начала рабочей смены и через 1,5–2 ч. после обеденного перерыва продолжительностью 15 мин. каждый или продолжительностью 10 мин. через каждый час работы;

– для 3 категории работ через 2 ч. от начала рабочей смены и через 1,5−2,0 ч. после обеденного перерыва продолжительностью 20 мин. каждый или продолжительностью 15 мин. через каждый час работы.

Во время регламентированных перерывов с целью снижения нервно эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления целесообразно выполнять комплексы упражнений для глаз, для улучшения мозгового кровообращения, для снятия утомления с плечевого пояса и рук, а также общего воздействия.

В случаях возникновения у пользователя зрительного дискомфорта и других неблагоприятных субъективных ощущений, несмотря на соблюдение санитарно-гигиенических, эргономических требований, режимов труда и отдыха следует применять индивидуальный подход в ограничении времени работ с ВДТ и ПЭВМ. Коррекцию длительности перерывов для отдыха или проводить смену деятельности на другую, не связанную с использованием ВДТ и ПЭВМ.

Организационные мероприятия, устраняющие причины возникновения пожаров: обучение рабочих и служащих противопожарным правилам, проведение лекций, инструкций и т.п. Технические мероприятия: соблюдение противопожарных правил и норм при устройстве оборудования отопления, вентиляции и т.д.

Мероприятия режимного характера: запрещение курения в не установленных местах, проведения сварочных работ в пожарных помещениях. Эксплуатационные мероприятия: правильная эксплуатация машин, транспорта, оборудования и правильное содержание зданий, территорий.

ВЫВОДЫ ПО ПЕРВОЙ ГЛАВЕ

В результате проведенного предпроектного обследования СЗИ ООО «Диалог-комплект», была проделана следующая работа:

– Составлен технический паспорт на автоматизированную систему обработки персональных данных;

– Разработана модель деятельности, отражающая процесс обработки информации ограниченного доступа;

– Разработан перечень персональных данных, подлежащих защите в автоматизированной системе обработки персональных данных;

– Разработана модель угроз безопасности персональных данных и произведена оценка их актуальности;

– Разработано техническое задание на создание системы защиты персональных данных на предприятии ООО «Диалог-комплект»;

– Был проведен анализ мероприятий по безопасности жизнедеятельности на предприятии ООО «Диалог-комплект».

2. ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ

2.1. Обзор возможных методов устранения уязвимостей

Для совершенствования защиты системы автоматизированной обработки персональных данных ООО «Диалог-комплект», были определены методы и средства, необходимые для устранения выявленных угроз и уязвимостей, определенных в первой главе данной работы, и выбраны из них наиболее эффективные варианты.

2.2. Угрозы несанкционированного доступа к информации

Согласно ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» [4] несанкционированный доступ (НСД) к информации – деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Одним из способов защиты от НСД является использование соответствующих программно-аппаратных средств, которые позволяют управлять доступом к автоматизированной системе, выполнять регистрацию и учет и обеспечивать целостность и неизменность программной среды.

В рамках ВКР был проведен сравнительный анализ программно-аппаратных средств защиты от НСД, результаты которого приведены в Таблицах 9 и 10.

Таблица 9 – Сравнение СЗИ от НСД

Критерии сравнения	Secret Net 7	Dallas Lock 8.0-K	Панцирь-К
Класс защищенности	По 3 классу защищенности	По 5 классу защищенности	По 5 классу защищенности
Уровень контроля НДВ	По 2 уровню контроля	По 4 уровню контроля	По 4 уровню контроля
Класс автоматизированных систем	До класса 1Б включительно	До класса 1Г включительно	До класса 1Г включительно
Дополнительные аппаратные требования: свободное место на жестком диске	2 Гб	0,03 Гб	0,02 Гб
Дополнительная аппаратая поддержка	есть	есть	есть
Цена, руб.	20 800 (вместе с ПАК «Соболь»)	17 900 (вместе с СДЗ «Dallas Lock»)	4 500

Таблица 10 – сравнение антивирусного ПО

Критерии сравнения	Kaspersky Endpoint Security 10 для Windows	ESET NOD32 Secure Enterprise Pack 5.0	Dr.Web Enterprise Security Suite
Наличие сертификата ФСТЭК	Классы Б2, В2, Г2	Классы А4, Б4, В4, Г4	Классы А2, Б2, В2
Наличие сертификата ФСБ	Классы Б2, В2, Г2	Нет	Классы А2, Б2, В2, Г2
Цена, руб.	2 000	2 725	5 850

На основании разработанной модели угроз угрозы, связанные с НСД были признаны актуальными. Для их минимизации были выбраны ПАК «Dallas Lock 8.0-К» с ПАК доверенной загрузки и антивирусное ПО «Kaspersky Endpoint Security 10 для Windows» из-за их выгодного соотношения цена/функциональность.

2.3. Угрозы преднамеренных действий внутренних нарушителей

Данные угрозы являются наиболее распространенными и, соответственно, наиболее важными с точки зрения защиты информации, так как больший приоритет имеет защита информации ограниченного доступа от преднамеренных действий внутренних нарушителей, а именно сотрудников, допущенных к ее обработке.

Для ООО «Диалог-комплект» актуален данный вид угроз и рекомендуются следующие меры для их минимизации:

– Установка СЗИ от НСД «Dallas Lock 8.0-К»;

– Установка антивирусного ПО «Kaspersky Endpoint Security 10 для Windows»;

– Обеспечение резервного копирования информации ограниченного доступа, обрабатываемой на АРМ.

2.4. Угрозы несанкционированного доступа по каналам связи

Данный вид угроз заключается в передаче запросов сетевым узлам и анализе ответов на них, в результате чего может быть получена топология сети, выявлены открытые уязвимые порты, используемые протоколы, активные сетевые сервисы.

В ходе анализа результатов предпроектного обследования было установлено, что для ООО «Диалог-комплект» угрозы несанкционированного доступа по каналам связи не актуальны.

ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ

На основе результатов работ по выявлению уязвимостей на рассматриваемом предприятии, приводящих к реализации возможных угроз, были применены следующие меры по их минимизации:

1. Для защиты от угроз несанкционированного доступа к информации:
   – Установлены СЗИ от НСД «Dallas Lock 8.0-K» и ПАК доверенной загрузки «Dallas Lock» по причине наилучшего соотношения цена/функциональность из сравниваемых СЗИ от НСД в Таблице 9;
   – Установлено антивирусное ПО «Kaspersky Endpoint Security 10 для Windows», так как его соотношение цена/функциональность, гораздо лучше, чем у конкурирующего антивирусного ПО;
2. Для защиты от угроз преднамеренных действий внутренних нарушителей:
   – Обеспечено резервное копирование информации, обрабатываемой на АРМ;
   – Установлены СЗИ от НСД «Dallas Lock 8.0-K» и ПАК доверенной загрузки «Dallas Lock»;
   – Установлено антивирусное ПО «Kaspersky Endpoint Security 10 для Windows»;

3. РАЗРАБОТКА ПРОЕКТА СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ ООО «ДИАЛОГ-КОМПЛЕКТ»

3.1. Описание объекта

ООО «Диалог-комплект» осуществляет поставки запасных частей к карьерному автомобилю БелАЗ в основные горнодобывающие регионы страны, из-за этого возникает большой объем информации, требующей защиты. В Таблице 12 представлены потоки защищаемой информации.

Таблица 11 – Потоки защищаемой информации

Входящая информация	Исходящая информация
Информация о клиентах	База данных клиентов

3.2. Резюме проекта

Разработка проекта велась согласно утвержденному техническому заданию на создание системы защиты персональных данных на предприятии ООО «Диалог-комплект» (Приложение Б).

Создание системы защиты должно осуществляться с помощью организационных, инженерно-технических и программно-аппаратных мер. На каждый конкретный этап работ должны быть назначены ответственные лица с помощью матрицы ответственности.

Результатом работ должна стать система защиты персональных данных ООО «Диалог-комплект», соответствующая нормативно-правовым актам в области защиты персональных данных.

3.3. Цели и задачи проекта

Целями создания системы защиты персональных данных ООО «Диалог-комплект» являются:

– Предотвращение угроз, связанных с НСД;

– Предотвращение угроз преднамеренных действий внутренних нарушителей;

– Предотвращение угроз несанкционированного доступа по каналам связи;

– Осуществление защиты персональных данных в соответствии с нормативно-правовыми актами.

3.4. Объекты поставки проекта

3.4.1. Организационно-распорядительная документация

Организационно-распорядительная документация на предприятии ООО «Диалог-комплект»:

– Инструкция по антивирусной защите (Приложение Г);

– Перечень персональных данных, подлежащих защите в автоматизированной системе обработки персональных данных (Приложение В);

– Технический паспорт на автоматизированную систему обработки персональных данных (Приложение А);

– Техническое задание на создание системы защиты персональных данных (Приложение Б);

– Модель деятельности (Приложение Ж);

– Инструкции администратору;

– Инструкция по парольной защите;

– Инструкция по резервированию;

– Журнал учета лиц;

– Журнал учета машинных носителей.

3.4.2. Программно-аппаратные и инженерно-технические меры

В рамках реализации проекта по созданию системы защиты персональных данных должны быть закуплены и установлены следующие программно-аппаратные средства:

– СЗИ от НСД «Dallas Lock 8.0-K»;

– Антивирусное ПО «Kaspersky Endpoint Security 10 для Windows»;

– ПАК доверенной загрузки «Dallas Lock»;

3.4.3. Обучение персонала

В рамках реализации проекта по созданию системы защиты персональных данных должно быть проведено обучение сотрудников порядку работы с персональными данными, обучение основам работы с СЗИ от НСД и инструктаж по антивирусной защите.

3.5. Риски проекта

Вероятность реализации угрозы через данную уязвимость в течение года: P(V), (%).

Критичность реализации угрозы через уязвимость: ER, (%).

Уровень угрозы Th (%), рассчитывается по Формуле (1):

$$Th = \frac{ER \cdot P(V)}{10000} \quad (1)$$

Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза CTh (%), рассчитывается по Формуле (2):

$$CTh = 1 - \prod_{i=1}^{n}(1 - Th) \quad (2)$$

Таблица 12 – Риски проекта

Риски / пути их реализации	Критичность ER	Вероятность P(V)	Th	CTh
1. Риски изменений в стране, обществе				
1.1. Ухудшение политических и экономических характеристик и факторов				0,0323
– реформы в экономике и политике	15	5	0,0075	
– изменение законодательства	25	10	0,025	
1.2. Изменение характеристик общества				0,1162
– здравоохранение и медицина	25	5	0,0125	
– возникновение негативного отношения сотрудников	70	15	0,105	
1.3. Влияние форс-мажорных обстоятельств				0,0025
– стихийные бедствия и природные катаклизмы	5	5	0,0025	
2. Риски окружения проекта в составе организации				
2.1. Изменение или недостаток бюджета проекта				0,8328
– задержки финансирования	80	15	0,12	
– отсутствие денежного резерва для реагирования на события рисков (в т.ч. для ликвидации отставания от графика)	90	90	0,81	
2.2. Недостаточная организованность работ				0,0733
– срыв графиков работ, невыполнение сроков	15	20	0,03	
– нехватка рабочей силы	20	5	0,01	
– недооценка стоимости работ и использование финансов для других целей	35	10	0,035	
2.3. Риски персонала				0,035
– влияние личностных факторов (неумеренные амбиции участников проекта, переоценка собственных возможностей, преувеличение роли технологической стороны в ущерб менеджменту)	20	5	0,01	
– риск недоступности персонала, которому сложно подобрать замену (болезнь, увольнение и другие непредвиденные обстоятельства)	25	10	0,025	

Минимальную угрозу проекту составляют риски стихийных бедствий и природных катаклизмов, а максимальную – риски изменения или недостатка бюджета проекта. Максимальные риски принимаются, так как устранить их невозможно.

3.6. Структура разбиения работ

Структура разбиения работ позволяет определить, какие работы необходимо выполнить для реализации проекта, и установить единую структуру управления этими работами. Структура разбиения работ представлена на Рисунке 1.

ИСПДн 1. Проектирование;

ИСПДн 1.1. Определение ключевых показателей существующих бизнес-процессов с точки зрения ИБ;

ИСПДн 1.2. Анализ проблем и слабых мест существующих бизнес процессов;

ИСПДн 1.3. Разработка значений ключевых показателей новых бизнес-процессов;

ИСПДн 1.4. Анализ и выбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов;

ИСПДн 1.5. Разработка и согласование структуры новых бизнес-процессов.

ИСПДн 2. Совершенствование организационно-распорядительной документации;

ИСПДн 2.1. Технический паспорт;

ИСПДн 2.2. Инструкция по антивирусной защите;

ИСПДн 2.3. Согласование и утверждение ОРД.

ИСПДн 3. Подготовка реализации проекта создания системы защиты персональных данных;

ИСПДн 3.1. Определение ответственных лиц и исполнителей проекта;

ИСПДн 3.2. Приобретение СЗИ от НСД;

ИСПДн 3.3. Приобретение ПАК доверенной загрузки;

ИСПДн 3.4. Приобретение антивирусного ПО.

ИСПДн 4. Внедрение;

ИСПДн 4.1. Установка и настройка СЗИ от НСД;

ИСПДн 4.2. Установка и настройка ПАК доверенной загрузки;

ИСПДн 4.3. Установка и настройка антивирусного ПО;

ИСПДн 4.4. Обучение пользователей;

ИСПДн 4.5. Контроль защищенности.

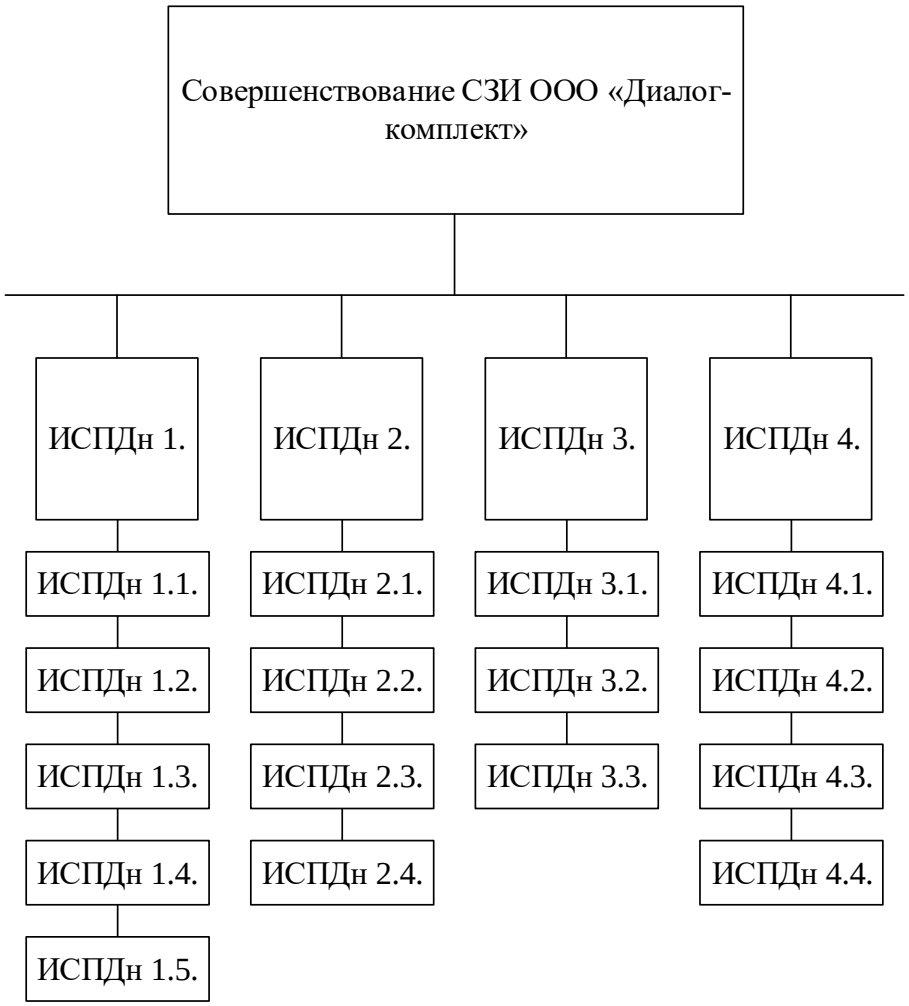


Рисунок 1 – Структура разбиения работ

3.7. Структурная схема организации проекта

Структурная схема организации проекта создания системы защиты персональных данных приведена на Рисунке 2.

Рисунок 2 – Структурная схема организации проекта

3.8. Матрица ответственности

Для наглядности обязанностей исполнителей проекта составляется матрица ответственности (Рисунок 3). Работа исполнителей разделяется на следующие группы: управление (У), исполнение (И), контроль (К).

Таблица 13 – Матрица ответственности

Исполнитель/Работа	1	2	3	4
ИСПДн 1.	К/У			
ИСПДн 1.1.	К		И	
ИСПДн 1.2.	К		И/К	
ИСПДн 1.3	К		И/К	
ИСПДн 1.4.	К		И	
ИСПДн 1.5.	К		И/К	
ИСПДн 2.	К		У/И	
ИСПДн 2.1.	К		У/И	
ИСПДн 2.2.	К		У/И	
ИСПДн 2.3.	К		У/И	
ИСПДн 2.4.	К		У/И	
ИСПДн 3.	К			
ИСПДн 3.1.	К			
ИСПДн 3.2.	К			
ИСПДн 3.3.	К			
ИСПДн 4.	К			
ИСПДн 4.1.	К	И		
ИСПДн 4.2.	К	И		
ИСПДн 4.3.	К	И		
ИСПДн 4.4.	К			И

3.9. Диаграмма Ганта и сетевой график

Диаграмма Ганта – инструмент для наглядной иллюстрации календарного плана разных этапов работ в проектном менеджменте. Для проекта создания системы защиты персональных данных ООО «Диалог-комплект». Диаграмма Ганта представлена в Приложении Д. На основании диаграммы Ганта проект займет 74 дня.

Сетевой график – это динамическая модель проекта, отражающая последовательность и зависимость работ, необходимых для завершения проекта. Сетевой график проекта создания системы защиты персональных данных на предприятии ООО «Диалог-комплект» представлен в Приложении Е.

3.10. Расчет бюджета проекта и его эффективности

Для устранения уязвимостей, выявленных в ходе предпроектного обследования, необходимо создание системы защиты обработки персональных данных ООО «Диалог-комплект». Был проведен расчет затрат на реализацию предложенных мер защиты. Стоимость оборудования и программного обеспечения приведена в Таблице 14. Стоимость реализации проекта приведена в Таблице 15. Чистая приведенная стоимость проекта представлена в Таблице 16.

Таблица 14 – Стоимость оборудования и программного обеспечения

Наименование	Количество	Цена за шт. (руб.)	Сумма (руб.)
СЗИ от НСД «Dallas Lock 8.0-K»	1	7 500	7 500
ПАК доверенной загрузки «Dallas Lock»	1	10 400	10 400
Антивирусное ПО «Kaspersky Endpoint Security 10 для Windows»	1	2 000	2 000
		Итог	19 900

Таблица 15 – Стоимость реализации проекта

Наименование	Стоимость (руб.)
Анализ существующей СЗИ	22 000
Разработка организационно-распорядительной документации	15 000
Установка и настройка СЗИ от НСД «Dallas Lock 8.0-K»	11 000
Установка и настройка ПАК доверенной загрузки «Dallas Lock»	5 500
Установка и настройка антивирусного ПО «Kaspersky Endpoint Security 10 для Windows»	4 200
Итог	57 700

Затраты на реализацию проекта совершенствования СЗИ на предприятии ООО «Диалог-комплект» составили 77 600 рублей.

Чтобы определить, будет успешным тот или иной проект финансовыми специалистами используется определенный метод оценки проектов – NPV.

Таблица 16 – Чистая приведенная стоимость проекта

Периоды	0	1	2	3	4
Первоначальные инвестиции	-77 600				
Выгоды		9 542 613	9 542 613	9 542 613	9 542 613
Стоимость годовой поддержки			-7 000	-7 000	-7 000
Затраты на поддержание инфраструктуры			-10 000	-10 000	-10 000
Итого	-77 600	9 542 613	9 525 613	9 525 613	9 525 613

NPV — это сокращение по первым буквам фразы «Net Present Value» и расшифровывается это как чистая приведенная (к сегодняшнему дню) стоимость. Это метод оценки инвестиционных проектов, основанный на методологии дисконтирования денежных потоков. Рассчитывается NPV по Формуле (3):

$$NPV = \sum_{t=0}^{n} \frac{CF_t}{(1+R)^t}, \quad (3)$$

где CF – денежный поток;
R – стоимость капитала (ставка дисконтирования);
n, t – количество временных периодов.

Ставку дисконтирования примем эквивалентной ключевой ставке центрального банка – 9,25 %.

NPV = 9542613⁄1,0925 + 9525613⁄$1,0925^2$ + 9525613⁄$1,0925^3$ + 9525613⁄$1,0925^4$ = = 8734657.2 + 7980866.42 + 7305140.9 + 6686627.82 = 30707292.34

Так как NPV больше нуля, значит данный проект создания системы защиты персональных на предприятии ООО «Диалог-комплект» выгоден.

ВЫВОДЫ ПО ТРЕТЬЕЙ ГЛАВЕ

В результате выполненных работ по реализации проекта по созданию системы защиты персональных данных ООО «Диалог-комплект» было сделано:

– Подготовлен комплект организационно-распорядительной документации;

– Закуплены и установлены программно-аппаратные средства защиты информации;

– Проведено обучение сотрудников порядку работы с персональными данными, обучение основам работы с СЗИ от НСД и инструктаж по антивирусной защите;

– Были рассчитаны риски проекта и определены их максимальные и минимальные значения;

– Было проведено разбиение работ и на его основе составлена матрица ответственности;

– Была построена диаграмма Ганта и сетевой график;

– Был проведен расчет бюджета проекта и его эффективности.

ЗАКЛЮЧЕНИЕ

В результате проведения выпускной квалификационной работы был проведен анализ состояния защиты информации на предприятии ООО «Диалог-комплект». В ходе предпроектного обследования были выявлены уязвимости в существующей системе защиты информации и отсутствие части организационно-распорядительной документации в области защиты информации. По этой причине были разработаны необходимые организационно-распорядительные документы и установлены программно-аппаратные средства защиты информации.

Результатами выпускной квалификационной работы стали:

– Разработан технический паспорт на автоматизированную систему – был проведен осмотр помещений и технических средств, составлены их перечни и схемы расположения;

– Разработана модель деятельности предприятия – построены диаграммы, позволяющие выявить потоки защищаемой информации;

– Разработана модель угроз и уязвимостей для автоматизированной системы и рассчитаны риски на основе базовой модели угроз безопасности ФСТЭК и методики определения актуальных угроз ФСТЭК;

– Разработано техническое задание на модернизацию системы защиты информации на предприятии ООО «Диалог-комплект»;

– Проведена оценка экономической эффективности проекта, по ее результатам внедрение системы защиты экономически целесообразно.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (выписка): утверждена заместителем директора ФСТЭК России 15.02.2008 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.
2. ГОСТ 34.602-1989. Техническое задание на создание автоматизированной системы. – М.: Изд-во стандартов, 1990. – 12 с.
3. ГОСТ Р 12.1.019-2009. Система стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты. – М.: Изд-во стандартов, 2010. – 32 с.
4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2008–02–01. – М.: Госстандарт России, 2001. – 12 с.
5. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – М.: Изд-во стандартов, 2009. – 40 с.
6. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»: утверждена заместителем директора ФСТЭК России 14.02.2008 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.
7. Постановление правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»: постановление правительства Российской Федерации от 01.11.2012 № 1119 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.
8. Приказ «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»: приказ ФСТЭК России от 18.02.2013 № 21 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.
9. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»: утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.
10. СанПин 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и огранизации работы. – М.: Изд-во стандартов, 2003. – 36 с.
11. СанПин 2.2.2.542-96. Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы. – М.: Изд-во стандартов, 1996. – 11 с.

12. СанПин 2.2.4.3359-16. Санитарно-эпидемологические требования к физическим факторам на рабочих местах. – М.: Изд-во стандартов, 2016. – 72 с.

13. «Стратегия национальной безопасности Российской Федерации до 2020 года»: утверждена Указом Президента Российской Федерации от 12.05.2009 № 537: // КонсультантПлюс. Технология 3000: Версия Проф [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.

14. «Стратегия развития информационного общества»: утверждена Указом Президента от 07.02.2008 № Пр-212: // КонсультантПлюс. Технология 3000: Версия Проф [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.

15. Федеральный закон «Об информации, информационных технологиях и защите информации»: федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ: // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.

16. Федеральный закон «О персональных данных»: федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.

17. ФГОС ВПО по направлению подготовки 090900 «Информационная безопасность». – Министерства образования и науки Российской Федерации, 2009. – 21с.

ПРИЛОЖЕНИЕ А

УТВЕРЖДАЮ
Генеральный директор Общества с ограниченной ответственностью «Диалог-комплект»

_____
«____» _____ 2016 г.

ТЕХНИЧЕСКИЙ ПАСПОРТ
на объект информатизации
АС «КЛИЕНТЫ»

Общества с ограниченной ответственностью «Диалог-комплект»

СОСТАВИЛ

_____ А.Л. Колпаков

«____» _____ 2016 г.

2016 г.

1 ОБЩИЕ СВЕДЕНИЯ ОБ ОБЪЕКТЕ

1.1 Наименование объекта: АС «КЛИЕНТЫ» Общества с ограниченной ответственностью «Диалог-комплект».

1.2 Расположение объекта: Челябинская обл., г. Челябинск, ул. Новоэлеваторная, д. 49, 2 этаж, кабинет № 210.

1.3 Классификация объекта: класс защищенности АС – 1Г, «Акт классификации…» Уч. № 000 от 01.11.2016 г.

2 СОСТАВ ОБОРУДОВАНИЯ ОБЪЕКТА

2.1 Состав основных технических средств и систем (ОТСС) объекта информатизации отражен в таблице 2.1.

Таблица 2.1 – Перечень ОТСС, входящих в состав ОИ АС «КЛИЕНТЫ»

Наименование устройства	Фирма производитель, модель	Заводской / инвентаризационный номер	Расположение
Системный блок	InWin	16112060900152	Рисунок 2.1
НЖМД	WD WD3200AAKX-001CA0	WD-WCAYUAA20921	Рисунок 2.1
Монитор	LG L1942S-BF	907NDBP3G709	Рисунок 2.1
Клавиатура	Genius K639	ZM7902171374	Рисунок 2.1
Мышь	A4-Tech OP-620D	0907	Рисунок 2.1
Принтер	HP LaserJet 1018	CNC1L86960	Рисунок 2.1
ИБП	APC SmartuPS 500	QS0614121487	Рисунок 2.1

2.2 Состав вспомогательных технических средств и систем (ВТСС) объекта, установленных в помещении объекта информатизации отражен в таблице 2.2.

Таблица 2.2 – Перечень ВТСС ОИ АС «КЛИЕНТЫ»

Наименование устройства	**Фирма производитель, модель**	**Заводской / инвентаризационный номер**	**Расположение**
Системный блок	InWin	619G109000187	Рисунок 2.2
Монитор	Samsung SyncMaster 720 NA	GS17HVFLA00045F	Рисунок 2.2
Клавиатура	Oklick 320M	3922302126	Рисунок 2.2
Мышь	Genius GM-0003A	X62405206687	Рисунок 2.2
МФУ	Canon MF3110	VZN81841	Рисунок 2.2
Системный блок	InWin	16221034300108	Рисунок 2.2
Монитор	LG	BEJE2241SX	Рисунок 2.2
Клавиатура	Logitech-k200	SY1464K	Рисунок 2.2
МФУ	HP LaserJet M1005MFP	CNG87CKHUF	Рисунок 2.2
Мышь	Logitech B110	LZ137HR21NP	Рисунок 2.2
Телефонный аппарат	LG GS0472H		Рисунок 2.2
Телефонный аппарат	LG GS0472H		Рисунок 2.2
Крипто-маршрутизатор	АПКШ континент	CH010105	Рисунок 2.2
Датчик пожарной сигнализации	б/н		Рисунок 2.2
Датчик пожарной сигнализации	б/н		Рисунок 2.2
Коммутатор	D-link DES-1005D	B12D449021069	Рисунок 2.2

2.3 Схема размещения и расположения ОТСС на объекте с привязкой к границам контролируемой зоны.

Структура, топология и размещение ОТСС и ВТСС объекта относительно границ контролируемой зоны объекта приведены на рисунках 2.1 – 2.3.

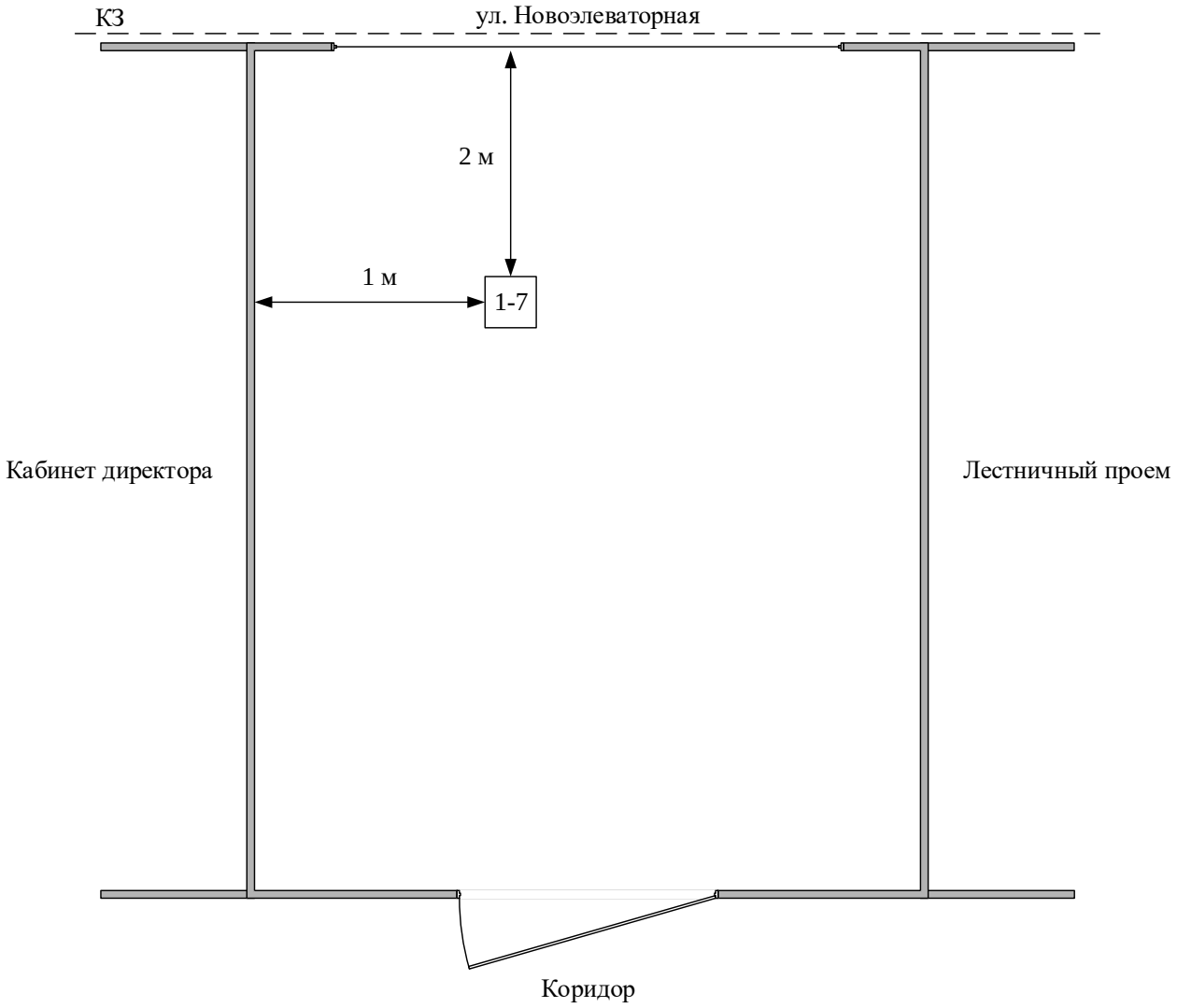


Рисунок 2.1 – Размещение ОТСС АС «КЛИЕНТЫ»
*Примечание: Обозначения 1-7 приведены в Таблице 2.1 основной части технического паспорта.

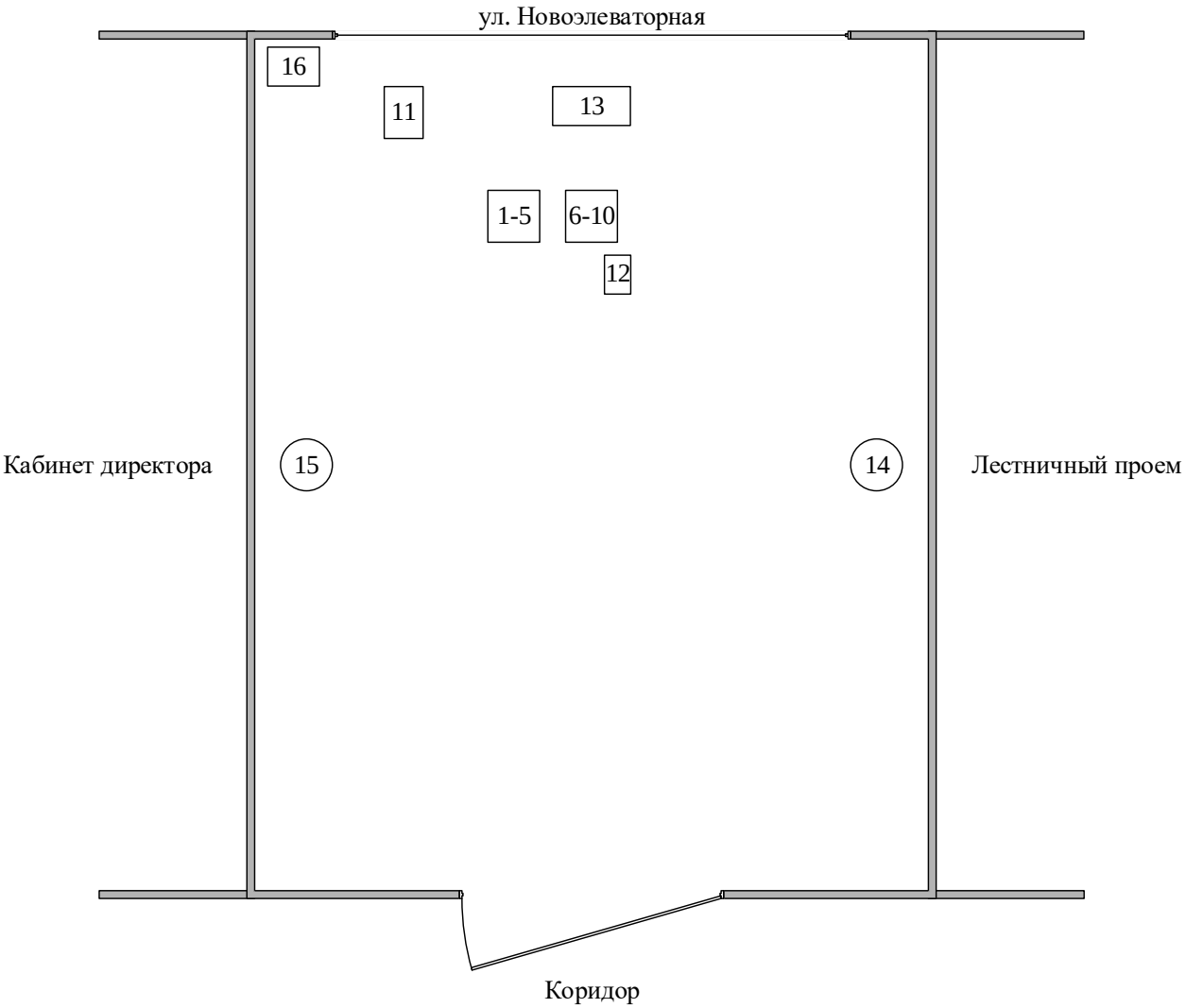
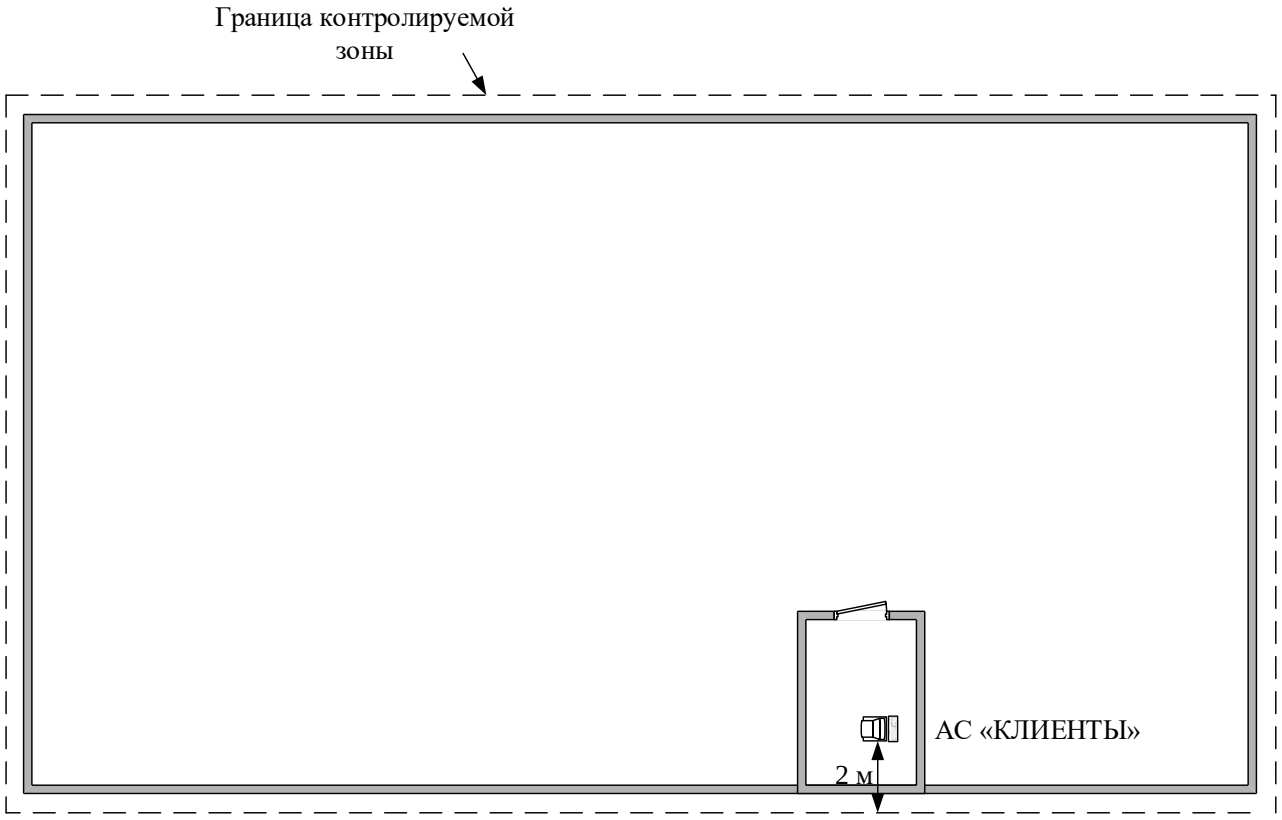


Рисунок 2.2 – Размещение ВТСС АС «КЛИЕНТЫ»
*Примечание: Обозначения 1-16 приведены в Таблице 2.2 основной части технического паспорта.



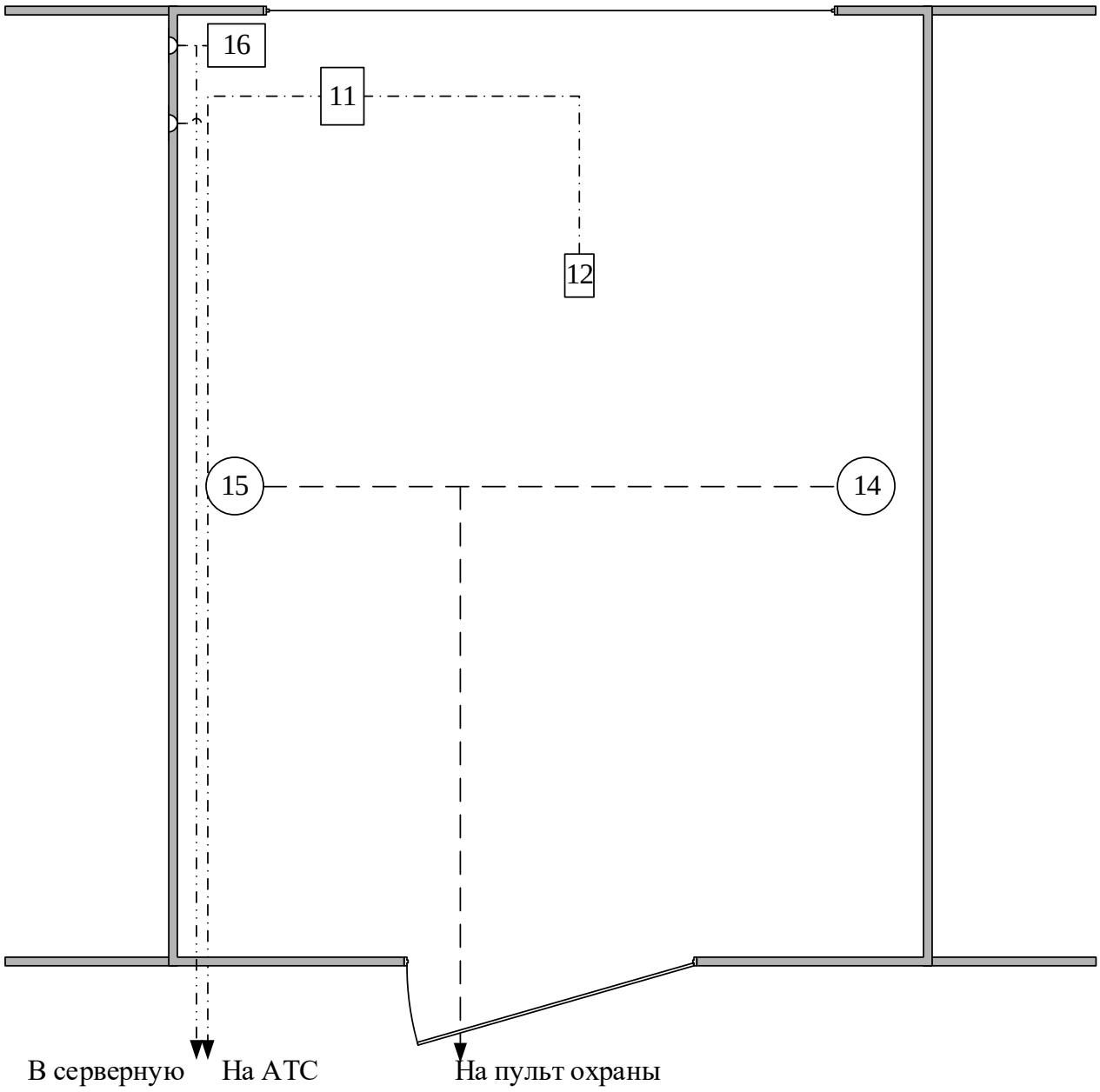
2 этаж ООО «Диалог-комплект» Челябинская обл.,
г. Челябинск, ул. Новоэлеваторнаяя, д. 49а

Рисунок 2.3 – Размещение ОТСС относительно границ контролируемой зоны

Границей контролируемой зоны являются ограждающие конструкции здания Общества с ограниченной ответственностью «Диалог-комплект» Челябинская обл., г. Челябинск, ул. Новоэлеваторная, д. 49 согласно приказу «Об определении границ контролируемой зоны объекта информатизации АС «КЛИЕНТЫ» № 77 от 11.02.2016 г.

Кабинет располагается на втором этаже. Окно выходит на ул. Новоэлеваторная, завешано жалюзи. Минимальное расстояние от ОТСС до КЗ составляет 2 метра.

2.4 Размещение ВТСС, линий приведено на рисунке 2.4.



Условные обозначения

— — — - Линия ОПС

_ . _ . _ . _ Линия телефонной связи

_ . . _ . . _ Линия ЛВС

Рисунок 2.4 – Размещение ВТСС, расположение линий

*Примечание: Обозначения 11-16 приведены в Таблице 2.2 основной части технического паспорта

2.5 Размещение системы электропитания, заземления и инженерных коммуникаций приведено на рисунке 2.5.

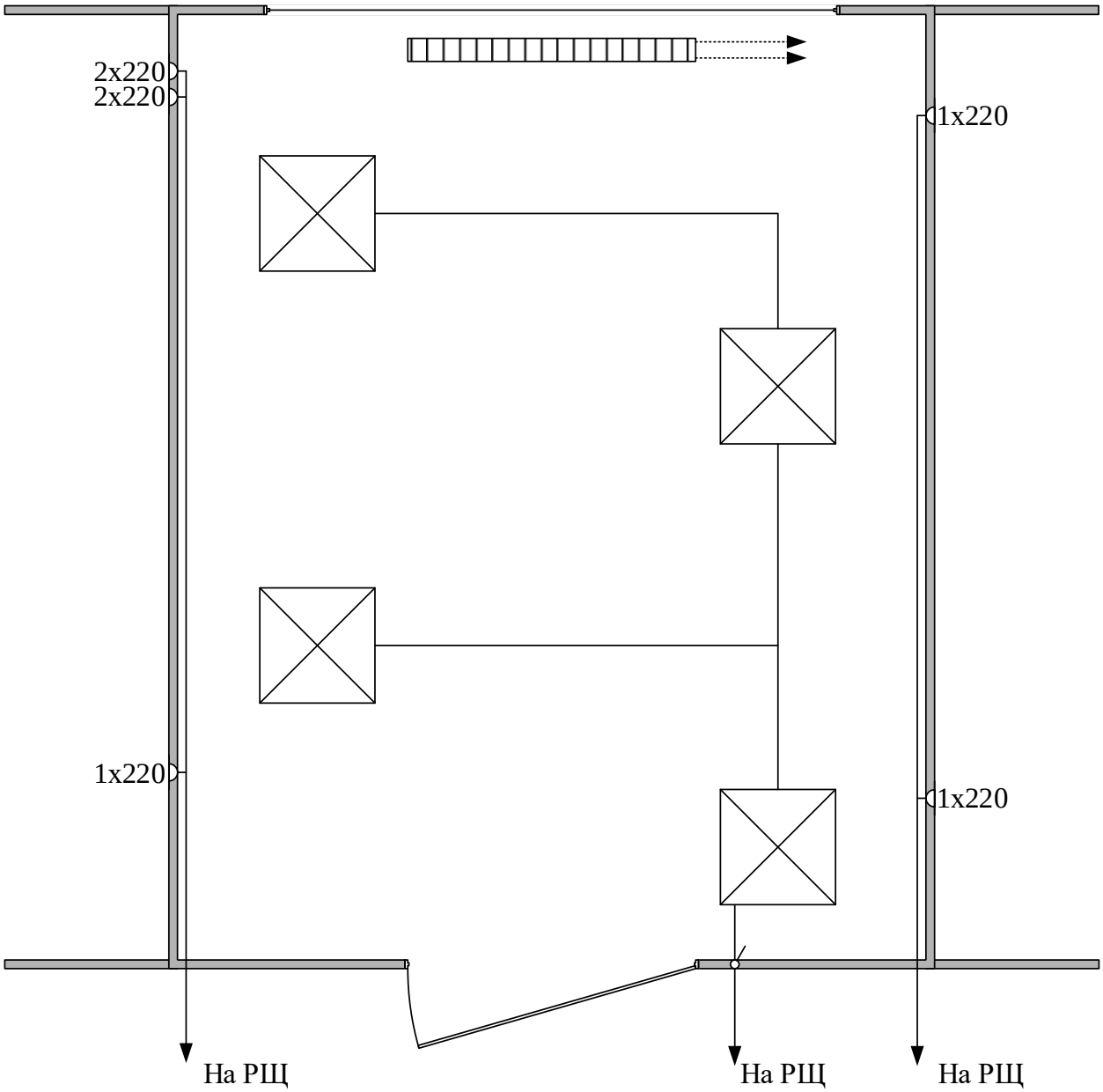


Рисунок 2.5 – Размещение системы электропитания, заземления и инженерных коммуникаций

Наименование линии	**Выходит за пределы КЗ (выходит/не выходит)**
Линия электропитания	не выходит
Линия заземления	не выходит
Линия охранной сигнализации	не выходит
Линия пожарной сигнализации	не выходит
Линия телефонной связи	выходит
Линия ЛВС	выходит
Линия отопления	выходит
Линия вентиляции	не выходит

2.6 Перечень средств защиты информации, установленных на объекте информатизации АС «КЛИЕНТЫ» приведен в Таблице 2.3.

Таблица 2.3 – Перечень средств защиты, установленных на ОИ АС «КЛИЕНТЫ»

Наименование и тип технического средства	Заводской номер/СЗЗ	Сведения о сертификате	Расположение
СЗИ от НСД «Dallas Lock 8.0-K»		№ 2720 действ. до 25.09.2018 г.	В ПЭВМ
Антивирусное ПО «Kaspersky Endpoint Security 10 для Windows»		№ 3025 действ. до 25.11.2019 г.	В ПЭВМ
МЭ АПКШ «Континент» версия 3.7		№ СФ/525-2948 действ. до 19.05.2017 г.	В ПЭВМ

2.7 Перечень программных средств, установленных на объекте информатизации АС «КЛИЕНТЫ» приведен в Таблице 2.4.

Таблица 2.4 – Перечень ПО установленного на ОИ АС «КЛИЕНТЫ»

Наименование ПО	Версия
Microsoft Windows 7 Professional SP1	6.1.7601.17514
7-zip	9.20.00.0
DallasLock 8.0-K	8.0.347.4
Kaspersky Endpoint Security 10 для Windows	10.2.5.3201
АРМ «Феанор»	10.63
КриптоПро CSP	3.9.8171

3 СВЕДЕНИЯ ОБ АТТЕСТАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1 Протоколы испытаний и даты их регистрации

3.2 Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации:

Заключение по результатам аттестационных испытаний объекта информатизации №

Аттестат соответствия №

4 УЧЕТ ПРОВЕДЕНИЯ РЕГЛАМЕНТНЫХ ПРОВЕРОК

Таблица 4.1 – Учет проведения регламентных проверок

Наименование организации, проводившей проверку	Дата проведения проверки	Номер протокола	Примечание

5 ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Таблица 5.1 – Лист регистрации изменения состава и размещения ОТСС, ВТСС и средств защиты объекта информатизации

Дата внесения изменений	Наименование документа, фиксирующего изменения	Номера заменённых (исправленных) листов формуляра	Подпись лица, внесшего изменения

ПРИЛОЖЕНИЕ Б

«УТВЕРЖДАЮ»
Генеральный директор
ООО «Диалог-комплект»
В.В. Ларионов
«___» _____2015 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на создание системы защиты персональных данных на предприятии ООО «Диалог-комплект»

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование системы и ее условное обозначение

Полное наименование системы: Система защиты автоматизированной системы обработки персональных данных, в обществе с ограниченной ответственностью «Диалог-комплект»

1.2. Наименование заказчика и исполнителя

Предприятие разработчик системы: ООО «Диалог-комплект», в лице главного специалиста по защите информации.

Предприятие заказчик системы: ООО «Диалог-комплект», в лице генерального директора.

1.3. Перечень документов, на основании которых создается система:

– Федеральный закон от 27 июля 2007 года N 152-ФЗ «О персональных данных»

– Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

– Трудовой кодекс РФ от 30.12.2001 N 197-ФЗ;

1.4. Порядок оформления и предъявления заказчику результатов работ по созданию системы (ее частей), по изготовлению и наладке отдельных средств (технических, программных, информационных) и программно-технических (программно-методических) комплексов системы

Результаты работы оформляются и предъявляются заказчику по мере исполнения в виде минимальных независимых частей проекта и/или предварительных проектов. Окончательный вариант проекта предоставляется на рассмотрение заказчику после главного специалиста по защите информации ООО «Диалог-комплект».

2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1. Назначение создания системы

В связи с постоянным ростом информационных потоков, соответственно растет и количество возможных угроз информационной безопасности. Для эффективного противодействия этим угрозам необходима система защиты персональных данных.

2.2. Цели создания системы

Основной целью проведения работ является приведение всех этапов работы с информации в автоматизированной системе обработки персональных данных ООО «Диалог-комплект» в соответствие требованиям перечисленных в данном Техническом задании.

3. ХАРАКТЕРИСТИКА ОБЪЕКТОВ ЗАЩИТЫ

3.1. Краткие сведения об объектах защиты

Объектом защиты является автоматизированная система обработки персональных данных, представляющая из себя автоматизированное рабочее место, носителей информации ограниченного доступа, помещение, в котором расположена автоматизированная система:

1. Автоматизированные рабочие места:
   - АРМ АС «КЛИЕНТЫ».
2. Помещения для хранения и работы с важной защищаемой информацией:
   - Кабинет главного бухгалтера.
3. Линии и средства связи, системы обеспечения функционирования СВТ и деятельности организации:
   - Линии проводной городской телефонной связи;
   - Система электропитания;
   - Линии охранной и пожарной сигнализации;
   - Линии локальной компьютерной сети.
4. Средства ввода-вывода и отображения информации:
   - Монитор главного бухгалтера;
   - Принтер HP LaserJet 1018;
   - Оперативная память ПК, входящего в АРМ.
5. Система бесперебойного питания АРМ:
   - Источник бесперебойного питания АРМ главного бухгалтера.
6. Носители информации:
   - Бумажные носители информации ограниченного доступа;
   - Электронные (CD/DVD диски, флэш-накопители с документами, содержащими информацию ограниченного доступа);
   - Персонал.
7. Персонал:
   - Генеральный директор;
   - Главный бухгалтер.

3.2. Сведения об условиях эксплуатации объекта защиты и характеристиках окружающей информационной среды

3.2.1. Объекты защиты подвержены воздействию следующих угроз:

3.2.1.1. АРМ:

- Уничтожение информации в случае повреждения носителей информаци;
- Несанкционированный доступ к информации в системе, хранящейся на АРМ.

3.2.2. Присутствуют следующие уязвимости:

3.2.2.1. АРМ:

- Отсутствие инструкции по эксплуатации СЗИ;
- Отсутствие описания технического процесса обработки информации ограниченного доступа;
- Отсутствие аппаратного модуля доверенной загрузки;

– Неактуальность актов категорирования и классификации объекта информатизации.

4. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

Работы должны проводиться в соответствии с положениями, перечисленными в данном Техническом задании.

Работы должны проводиться в два этапа: Приведение в соответствие с нормативно-правовыми актами порядка обработки персональных данных, проверка технических средств обработки информации.

4.1. Приведение в соответствие с нормативно-правовыми актами порядка обработки персональных данных

Список необходимых к проведению работ относительно автоматизированной системы обработки персональных данных:

– Разработка нормативно-правовой документации: Акта обследования АС, акта классификации АС, описания технологического процесса обработки информации, инструкции по эксплуатации СЗИ, технического паспорта;

– Изучение существующих организационных мер обеспечения безопасности информации ограниченного доступа;

– Разработка актуализированной модели угроз;

– Разработка перечня требований по защите информации ограниченного доступа;

– Выявление имеющихся средств технической защиты информации и мер, которые применяются для обеспечения безопасности персональных данных;

– Анализ соответствия применяющихся мер и средств технической защиты предъявляемым требованиям нормативно-правовой базы Российской Федерации в области защиты персональных данных.

4.2. Проверка технических средств обработки информации

Список необходимых к проведению работ относительно автоматизированной системы обработки персональных данных:

– Определение условий расположения технических средств обработки информации ограниченного доступа относительно границ контролируемой зоны;

– Определение линий и коммуникаций, расположенных в месте размещения технических средств обработки информации ограниченного доступа;

– Изучение существующих организационных мер обеспечения безопасности работоспособности и функционирования информационных систем;

– Покупка необходимых программных и технических средств, для обеспечения повышения защищенности автоматизированной системы;

– Обновление программных продуктов информационной системы до актуального состояния;

4.3. Порядок проведения работ:

4.3.1. Для выполнения работ Исполнитель привлекает специалистов Заказчика имеющих необходимую компетенцию.

4.3.2.

4.3.3. Специалисты Заказчика временно переходят под руководство Исполнителя.

4.3.4. В ходе проведения работ Исполнитель собирает исходные данные путем:

– опроса персонала Заказчика, в том числе руководителей и сотрудников структурных подразделений;

– обследования АРМ и места его расположения;

– анализа документов и записей результатов деятельности Заказчика в части обеспечения безопасности информационных систем персональных данных (нормативных документов, проектной и эксплуатационной документации, актов, журналов и пр.).

5. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ ГОТОВОЙ СИСТЕМЫ

5.1. Критериями для приемки работ является настоящее техническое задание и соответствующие частные Технические задания, разрабатываемые в процессе выполнения работ.

5.2. Приемка работ осуществляется единовременно.

5.3. Заказчик направляет замечания в письменном виде.

6. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ ПРОЕКТА РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА ЗАЩИТЫ К ВВОДУ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ДЕЙСТВИЕ

При подготовке к проведению Исполнителем работ со стороны Заказчика необходимо обеспечить следующее:

– назначить ответственное лицо от Заказчика, наделенное соответствующими полномочиями, для обеспечения выполнения работ Исполнителем;

– определить лицо для организации и проведения опроса;

– обеспечить промежутки времени доступности лиц, АРМ и выделенного помещения.

7. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

7.1. При разработке системы Исполнителем должны быть подготовлены следующие документы:

– Программа и методика испытаний объекта информатизации;

– Акт обследования автоматизированной системы;

– Акт классификации автоматизированной системы;

– Описание технического процесса обработки информации ограниченного доступа;

– Технический паспорт.

7.2. Отчетные документы предоставляются Заказчику в электронном виде в формате документов Microsoft Office и на бумажных носителях.

8. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ И ОГРАНИЧЕНИЯ

8.1. В случае поставки и внедрения технических средств защиты третьей стороной до начала работ по аттестации, Заказчик согласует с Исполнителем следующее:

– состав и спецификацию технических средств;

– состав сопроводительной документации к техническим средствам и сертификатов;
– схемы установки и подключения;
– настройки аппаратно-программных средств;
– рабочую документацию этапа внедрения.

8.2. Срок поставки и внедрения технических средств защиты не входит в расчет сроков этапов работ.

В случае задержки по срокам предоставления исходных данных при проведении работ, или неполного предоставления информации со стороны Заказчика, по согласованию сторон возможен перенос сроков выполнения работ по договору в сторону увеличения.

ПРИЛОЖЕНИЕ В

УТВЕРЖДАЮ

Генеральный директор ООО «Диалог-комплект»

_____В.В. Ларионов

«____»_____ 2017 г.

ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ,
подлежащих защите в автоматизированной системе обработки персональных данных
АС «КЛИЕНТЫ»

№	Тип персональных данных, подлежащих защите
1.	Фамилия, Имя, Отчество
2.	Паспортные данные
3.	Дата рождения
4.	Адреса проживания и прописки
5.	Сведения об образовании
6.	Учебное заведение
7.	Образовательное заведение
8.	Индивидуальный номер налогоплательщика
9.	Страховой номер индивидуального лицевого счета

Генеральный директор ООО «Диалог-комплект» _____ В.В. Ларионов

ПРИЛОЖЕНИЕ Г

УТВЕРЖДАЮ

Генеральный директор ООО «Диалог-комплект»

_____В.В. Ларионов

«____» _____ 2017 г.

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ
в автоматизированной системе обработки персональных данных
АС «КЛИЕНТЫ»

2017 г.

УСЛОВНЫЕ СОКРАЩЕНИЯ:

АВЗ – антивирусная защита;

ИСПДн – информационная система персональных данных;

ПДн – персональные данные.

1 ОБЩИЕ ТРЕБОВАНИЯ

1.1. Настоящая инструкция определяет требования к организации защиты автоматизированной системы обработки персональных данных АС «КЛИЕНТЫ» ООО «Диалог-комплект» (далее ИСПДн) от разрушающего воздействия компьютерных вирусов и иного вредоносного программного обеспечения и устанавливает ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.2. К использованию в ИСПДН допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.3. Установка и настройка средств антивирусного контроля на рабочих станциях ИСПДн осуществляется администратором или специально назначенным лицом в соответствии с руководствами по применению конкретных антивирусных средств.

1.4. Данные требования не распространяются на рабочие станции с установленными операционными системами, для которых отсутствуют какие-либо средства антивирусного контроля.

2 ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОГО КОНТРОЛЯ

2.1. Любой программный модуль перед запуском должен проходить автоматический антивирусный контроль. Для этого необходимо осуществлять проверку либо при загрузке компьютера всех дисков и файлов рабочих станций, либо непосредственно перед запуском конкретного программного модуля.

2.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.3. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), администратором защиты ИСПДн должна быть выполнена антивирусная проверка на защищаемых серверах и рабочих станциях.

2.4. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно или вместе с администратором защиты ИСПДн должен провести внеочередной антивирусный контроль своей рабочей станции.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИСПДн обязаны:

- приостановить работу в ИСПДн;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения и администратора защиты ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

3 ОТВЕТСТВЕННОСТЬ

3.1. Ответственность за организацию и проведение антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на администратора соответствующей информационной системы персональных данных.

3.2. Периодический контроль состояния антивирусной защиты в ИСПДн, а также соблюдения установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции осуществляется администратором за обеспечение безопасности персональных данных.

Генеральный директор ООО «Диалог-комплект» _____ В.В. Ларионов

С инструкцией ознакомлены:

№	ФИО	Подпись
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		

ПРИЛОЖЕНИЕ Д

Для построения диаграммы Ганта определим перечень поставленных задач и их сроки (с учетом выходных дней).

Таблица 1 – Перечень работ и сроков

Название работы	Длительность	Начало	Окончание
1. Проектирование	13	17.01.2017	30.01.2017
1.1. Определение ключевых показателей бизнес-процессов с точки зрения ИБ	2	17.01.2017	19.01.2017
1.2. Анализ проблем и слабых мест существующих бизнес-процессов	3	19.01.2017	22.01.2017
1.3. Разработка значений ключевых показателей новых бизнес-процессов	3	22.01.2017	25.01.2017
1.4. Анализ и выбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов	3	25.01.2017	28.01.2017
1.5. Разработка и согласование структуры новых бизнес-процессов	2	28.01.2017	30.01.2017
2. Совершенствование организационно-распорядительной документации	10	30.01.2017	09.02.2017
2.1. Технический паспорт	3	30.01.2017	02.02.2017
2.2. Инструкция по антивирусной защите	3	02.02.2017	05.02.2017
2.3. Согласование и утверждение ОРД	4	05.02.2017	09.02.2017
3. Подготовка реализации проекта создания системы защиты персональных данных	30	09.02.2017	11.03.2017
3.1. Определение ответственных лиц и исполнителей проекта	3	09.02.2017	12.02.2017
3.2. Приобретение СЗИ от НСД	7	12.02.2017	19.02.2017
3.3. Приобретение ПАК доверенной загрузки	10	19.02.2017	01.03.2017
3.4. Приобретение антивирусного ПО	10	01.03.2017	11.03.2017
4. Внедрение	21	11.03.2017	01.04.2017
4.1. Установка и настройка СЗИ от НСД	4	11.03.2017	15.04.2017
4.2. Установка и настройка ПАК доверенной загрузки	4	15.04.2017	19.04.2017
4.3. Установка и настройка антивирусного ПО	3	19.04.2017	22.04.2017
4.4. Контроль защищенности	3	22.04.2017	25.04.2017
4.5. Обучение пользователей	7	25.04.2017	01.04.2017

На основе этих данных мы можем построить диаграмму Ганта, представленную на Рисунке 1.

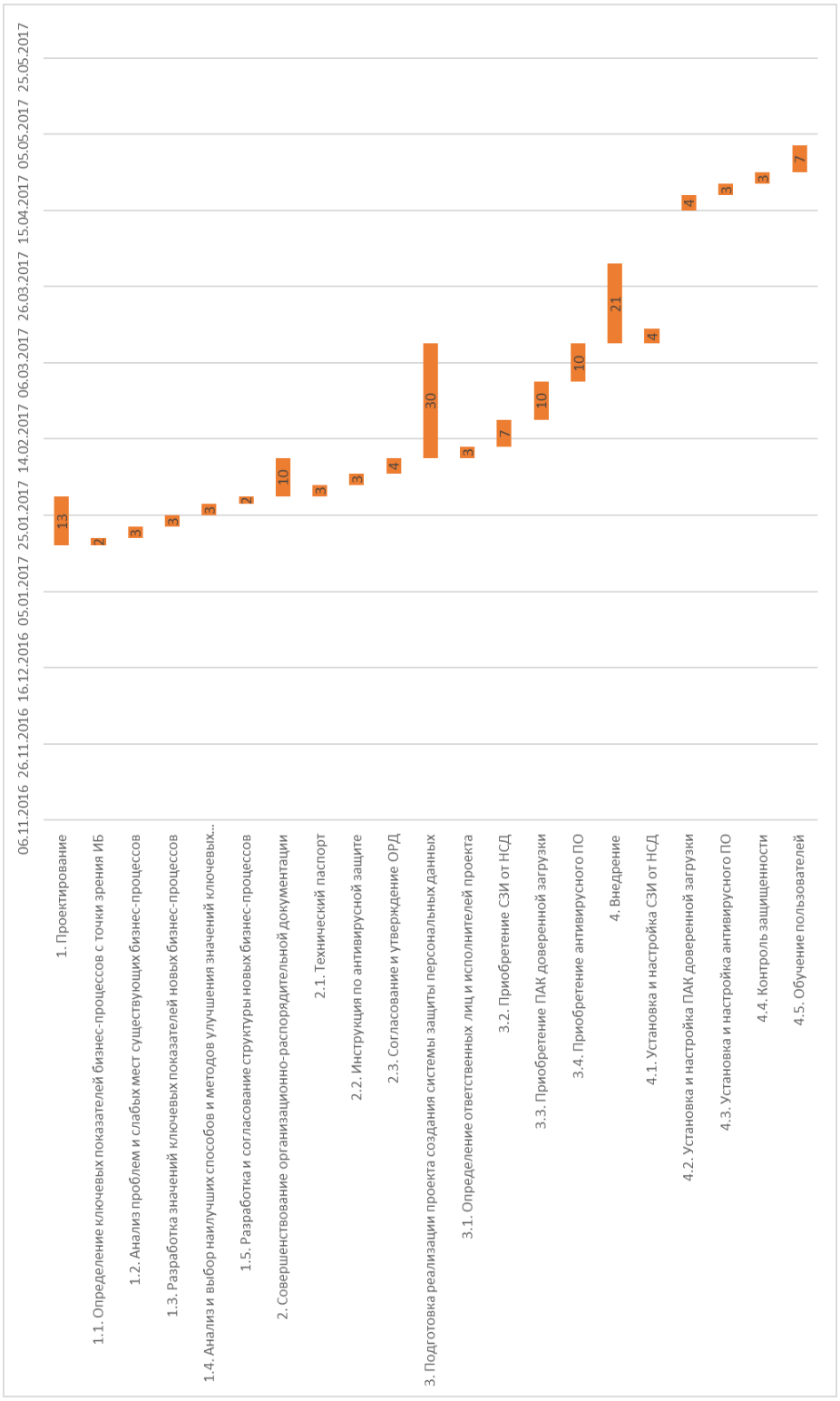


Рисунок 1 – Диаграмма Ганта

ПРИЛОЖЕНИЕ Е

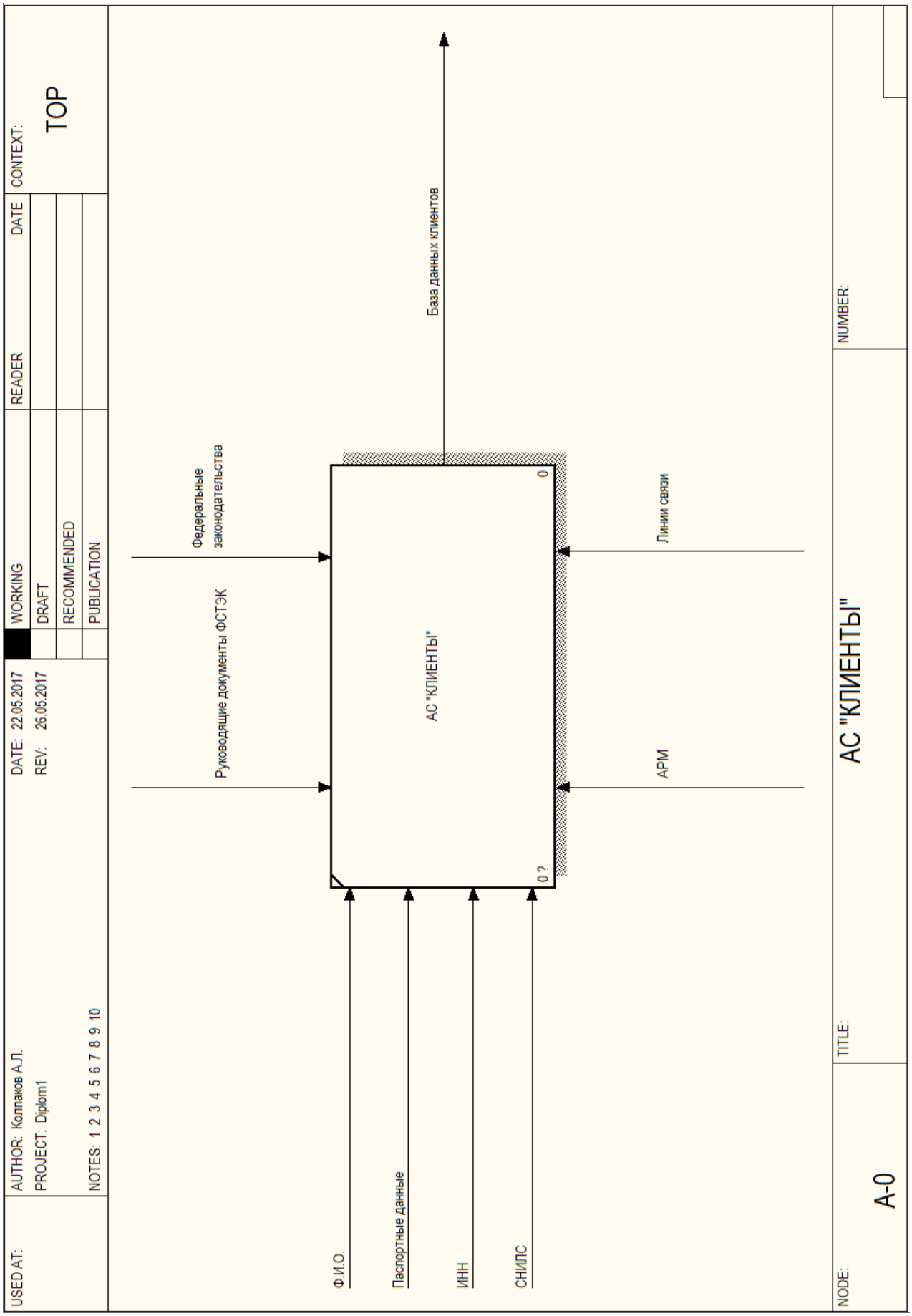
Для своевременного выполнения работ, а также соответствия плану работ необходимо определить сроки выполнения работ (Таблица 1).

i-j – код работы
T – длительность работы, дней
$T_{рн}$ – ранний срок начала работы
$T_{пн}$ – поздний срок начала работы
$T_{ро}$ – ранний срок окончания работы
$T_{по}$ – поздний срок окончания работы

Таблица 1– Расписание выполнения работ

i-j	Название работы	T	$T_{рн}$	$T_{пн}$	$T_{ро}$	$T_{по}$
	Проектирование	13	0	0	13	13
1-2	Определение ключевых показателей существующих бизнес-процессов с точки зрения ИБ	2	0	0	2	2
2-3	Анализ проблем и слабых мест существующих бизнес-процессов	3	2	2	5	5
3-4	Разработка значений ключевых показателей новых бизнес-процессов	3	5	5	8	8
4-5	Анализ и выбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов	3	8	8	11	11
5-6	Разработка и согласование структуры новых бизнес-процессов	2	11	11	13	13
	Совершенствование ОРД	10	13	13	23	23
6-7	Технический паспорт	3	13	13	16	16
7-8	Инструкция по антивирусной защите	3	16	16	19	19
8-9	Согласование и утверждение ОРД	4	19	19	23	23
	Подготовка реализации проекта создания системы защиты персональных данных	30	23	23	53	53
9-10	Определение ответственных лиц и исполнителей проекта	3	23	23	26	26
10-11	Приобретение СЗИ от НСД	7	26	26	33	33
11-12	Приобретение ПАК доверенной загрузки	10	33	33	43	43
12-13	Приобретение антивирусного ПО	10	43	43	53	53
	Внедрение	21	53	53	74	74
13-14	Установка и настройка СЗИ от НСД	4	53	53	57	57
14-15	Установка и настройка ПАК дов. загрузки	4	57	57	61	61
15-16	Установка и настройка антивирусного ПО	3	61	61	64	64
16-17	Обучение пользователей	3	64	64	67	67
17-18	Контроль защищенности	7	67	67	74	74

ПРИЛОЖЕНИЕ Ж



ПРИЛОЖЕНИЕ З

УТВЕРЖДАЮ
Генеральный директор ООО «Диалог-комплект»

_____В.В. Ларионов
«____» _____ 2017 г.

ООО «Диалог-комплект»

АКТ
присвоения уровня защищенности
автоматизированной системы обработки персональных данных
КЛИЕНТЫ»

Комиссия в составе: председатель – Генеральный директор ООО «Диалог-комплект» Ларионов В.В., члены комиссии – Специалист по защите информации Орлов М.М., Системный администратор Рыбаков Я.В., назначенная Генеральным директором ООО «Диалог-комплект», провела работу по определению и присвоению уровня защищенности ИСПДн «КЛИЕНТЫ».

Рассмотрев исходные данные об информационной системе персональных данных, определила:

1) категория персональных данных: Иные;
2) количество субъектов персональных данных: менее 100 000;
3) актуальные угрозы безопасности персональных данных, являются угрозами 3 типа;
4) наличие взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена: Сеть Интернет;

В соответствии с Постановлением «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 и на основании анализа исходных данных, РЕШИЛА:

информационной системе персональных данных «КЛИЕНТЫ» ООО «Диалог-комплект» присвоить уровень защищенности: УЗ-4.

Председатель комиссии _____ В.В. Ларионов

Члены комиссии _____ М.М. Орлов

_____ Я.В. Рыбаков